



Microsoft Intune

Dein ultimativer Guide zur Einrichtung und Administration

- Windows AutoPilot erfolgreich einrichten
- Endpoint Protection Baseline aufbauen
- iOS- und Android-Geräte administrieren 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](#)

 YOUTUBE [Aaron-Siller-YT](#)

Inhaltsverzeichnis

Einleitung	7
Kapitel 1 – Überblick: Microsoft Intune im Microsoft Cloud Security Stack	8
Kapitel 2: Planung der Geräteverwaltung und Architekturentscheidung in Microsoft Intune....	12
Kapitel 3: Geräteszenarien und Registrierungswege in Microsoft Intune	15
Übersicht über die Geräteszenarien	16
Registrierungswege: Was musst du beachten?	16
Aufwand und strategische Überlegungen	18
Grundsätzlicher Hinweis	19
Kapitel 4: Gerätbestand und Konformität – die Basis für eine saubere Verwaltung	19
Kapitel 5: App-Schutzrichtlinien als zusätzlicher Sicherheitslayer.....	21
Kapitel 6: Erweiterung der lokalen Infrastruktur in Microsoft Intune	23
Kapitel 7: Die verschiedenen Join-Typen in Entra ID und Intune.....	25
Entra ID Hybrid Joined	26
Entra ID Joined	27
Entra ID Registered.....	27
Kapitel 8: Office-Installationen im Microsoft 365 Admin Center verwalten und ungewollte Geräte-Registrierungen in Entra ID vermeiden.....	31
Nachverfolgung von Installationen	33
Zugriff auf Drittanbieterspeicher in Microsoft 365 on the Web einschränken.....	34
Cortana-Zugriff auf M365-Daten einschränken	35
Self Services für Benutzer deaktivieren	36
Externer Zugriff auf SharePoint, OneDrive und Teams: Gastfreigaben sinnvoll konfigurieren.	39
Vergleich der Freigabeoptionen für externe Benutzer in Microsoft 365	41
Hinweis zum Self-Service-Passwort-Reset	41
Kapitel 9: Gastkonten, Benutzerrechte und Gruppenverwaltung in Microsoft Entra ID	43
Benutzerrechte unter „User Settings“	44
Steuerung der Gruppenanlage.....	46
Ablaufdatum für Microsoft 365-Gruppen.....	47
Kapitel 10: Geräteeinstellungen und -registrierung in Microsoft Entra ID	49

Benutzer können Geräte mit Microsoft 365 verknüpfen.....	50
Benutzer können ihre Geräte bei Microsoft Entra registrieren	51
Multi-Faktor-Authentifizierung für Registrierung oder Join erforderlich	52
Gerätegrenzwerte, lokale Administratorrechte und Gerätetherche.....	53
Umgang mit lokalen Administratorrechten	54
Validierung von registrierten Geräten	55
Veraltete Geräte erkennen, deaktivieren und bereinigen	56
Kapitel 11: Benutzereinwilligungen und Schatten-IT kontrollieren	58
Analyse der vorhandenen Anwendungen.....	60
Kapitel 12: Plattformregistrierung in Intune einschränken.....	61
Kapitel 13: Windows Autopilot – Grundlagen und praktische Umsetzung	68
Kapitel 14: Zentrale Enrollment-Einstellungen und Windows Hello for Business in Intune	72
Kapitel 15: Windows Autopilot Deployment Profiles	77
Nutzung von dynamischen Gruppen	82
Konfiguration der Enrollment Status Page für AutoPilot-Deployments	85
Einsatz der Enrollment Status Page zur Steuerung der Applikationsbereitstellung	88
Manuelles Hochladen von Geräten in Windows Autopilot per PowerShell-Skript	91
Zuweisung von Autopilot-Profilen über Gruppentags und dynamische Gerätegruppen	93
Kapitel 16: Apple-Geräteverwaltung mit Intune und Apple Business Manager.....	98
Einbindung von Apple-Geräten, Zertifikatsverwaltung und Registrierungswege.....	99
Übersicht zur Geräte-Registrierung über Enrollment Types (iOS/iPadOS)	102
Webbasierte Registrierung von Apple-Geräten mit Intune (Just-in-Time Enrollment)	104
Account Driven User Registrierung von Apple-Geräten	108
Kapitel 17: Verwaltung von Apple-Geräten mit dem Apple Business Manager und dem Enrollment Program Token	111
Kapitel 18: Verwaltung von Android-Geräten mit Intune – Registrierungsarten und Geräteneigentum	118
Android-Geräteverwaltung mit Intune – Enrollment-Typen und QR-Code-basierte Registrierung	120
1. Corporate-owned Fully Managed User Devices	122

2. Corporate-owned Devices with Work Profile	122
Kapitel 19: Namenskonventionen, Domain Join und Geräteeigentum im Windows Autopilot Hybrid Join	127
Kapitel 20: Verwaltung von Apple IDs und Domainerfassung im Apple Business Manager.....	130
Kapitel 21: Gerätebereinigung und Compliance-Richtlinien in Microsoft Intune.....	133
Kapitel 22: Einführung in Conditional Access – Grundlagen und empfohlene Richtlinien.....	138
Kapitel 23: Config Refresh – Konfigurationssicherheit und Performancestabilisierung	141
Kapitel 24: BitLocker-Verschlüsselung und Konfigurationsunterschiede in Intune	143
Kapitel 25: OneDrive und der Known Folder Move (KFM)	146
Kapitel 26: Konfiguration der LAPS-Funktion in Microsoft Intune	147
Kapitel 27: Geräteeinschränkungen und ADMX-Import in Intune	151
Kapitel 28: Erweiterte Geräteinventarisierung mit dem Properties-Katalog in Intune	153
Kapitel 28: Managed Apps, Discovery Apps und Geräte-Diagnose in Intune	155
Kapitel 30: App-Schutzrichtlinien, Microsoft 365 Policies und Security Baselines in Intune.....	161
App Protection Policies – Data Protection und Access Requirements	168
Kapitel 31: Applikationsbereitstellung in Microsoft Intune	172
Erweiterte Applikationsverwaltung mit Apple VPP und Microsoft Store in Intune.....	174
Office App-Suite Bereitstellung mit Intune: Konfiguration über den Designer oder XML.....	177
Feinkonfiguration der Office App-Suite in Intune: Optionen, Versionen und Sprachpakete	179
Zuweisung und Bereitstellung von Applikationen in Intune: Grundlagen und Besonderheiten	181
Sonderfall: Microsoft Defender für Endpoint	183
Kapitel 32 – MSI- und Win32-App-Deployment mit Microsoft Intune	189
Auswahl des Apptyps im Intune-Portal.....	190
Upload der Intune-WIN-Datei und erste Konfiguration.....	193
Umgang mit individuellen Installationsparametern	202
Grundlagen und Werkzeuge der App-Paketierung in Intune.....	202
Tools, Dienste und Alternativen zur manuellen Paketierung.....	210
Kapitel 33: Reporting und Auswertung in Intune – Richtlinien, Compliance und Log-Analyse..	211

Kapitel 34: Remote-Support, Audit-Logs und Group Policy Analytics in Intune	217
Schlusswort: Dein Weg zu einer sicheren Microsoft 365 Umgebung.....	223

Einleitung

Microsoft Intune ist ein zentrales Werkzeug für die moderne Geräteverwaltung und Sicherheit in Unternehmen. Es ermöglicht dir, Windows-, Android- und iOS-Endgeräte einheitlich zu konfigurieren, zu schützen und zu verwalten – unabhängig davon, ob es sich um unternehmenseigene oder private Geräte handelt.

In vielen Umgebungen wird Intune bereits eingesetzt, aber nicht konsequent konfiguriert. Dabei ist klar: Ohne klare Richtlinien und Kontrolle bleiben Schwachstellen bestehen – Geräte können ungeschützt sein, Richtlinien greifen nicht, und Unternehmensdaten sind angreifbar.

Ziel dieses Leitfadens ist es, dir eine praxisorientierte, technische Grundlage zur Verfügung zu stellen, mit der du Intune professionell einsetzt und deine Geräteumgebung sicher verwaltest. Du erfährst unter anderem:

- wie du Geräterichtlinienbasiert registrierst und absicherst,
- wie du Betriebssystemplattformen gezielt zulässt oder blockierst,
- wie du Compliance-Richtlinien und Appschutzprofile konfigurierst,
- wie du Windows-Autopilot für die automatisierte Bereitstellung nutzt,
- wie du mit Endpoint Security und Geräteschutzrichtlinien arbeitest.

Dabei legen wir den Schwerpunkt auf reale Szenarien und konkrete Konfigurationen, die sich in produktiven Umgebungen bewährt haben. Die Inhalte basieren auf praktischen Schulungserfahrungen und aktuellen Entwicklungen im Microsoft Endpoint Management Umfeld.

Besonders wichtig ist ein **ganzheitlicher Ansatz**: Intune allein bietet viele Möglichkeiten – doch erst in Kombination mit Entra ID, Conditional Access und App-Konfigurationen entsteht eine wirkungsvolle Gesamtlösung. Nur so erreichst du ein hohes Maß an Sicherheit und gleichzeitig eine reibungslose Nutzererfahrung.

In diesem E-Book konzentrieren wir uns daher auf die technische Umsetzung in Microsoft Intune – Schritt für Schritt, mit Fokus auf Klarheit und Sicherheit.

Legen wir los.

Kapitel 1 – Überblick: Microsoft Intune im Microsoft Cloud Security Stack

Wenn wir über **Microsoft Intune** sprechen, bewegen wir uns innerhalb des sogenannten **Microsoft Cloud Security Stacks**. Intune ist dabei nur eines von mehreren Modulen, die gemeinsam eine umfassende Sicherheits- und Compliance-Architektur bilden.

Zentraler Startpunkt in diesem Stack ist die **Security und Compliance Policy Engine**. Bevor du irgendeine konkrete Konfiguration in Intune oder anderen Diensten vornimmst, musst du dir im Klaren darüber sein, welche Sicherheits- und Compliance-Maßnahmen in deinem Tenant umgesetzt werden sollen. Dazu zählen unter anderem:

- Welche Zugriffsmöglichkeiten willst du erlauben?
- Welche Ressourcen dürfen genutzt werden?
- Welche Geräte dürfen registriert werden?
- Welche Richtlinien sollen greifen?

Diese grundlegenden Überlegungen beeinflussen die gesamte nachgelagerte Administration und Konfiguration.

Wenn du den Blick auf die übergeordnete Struktur richtest, wirst du feststellen, dass wichtige Dienste wie **Microsoft Entra ID** und **Microsoft 365 Defender / Defender XDR** eng mit Intune verbunden sind:

- In **Entra ID** verwaltet du Benutzer, Gruppen, Geräte und App-Einstellungen.
- Ein zentrales Werkzeug dort ist **Conditional Access**.

Mit Conditional Access kannst du granulare Zugriffsrichtlinien definieren und so sicherstellen, dass Registrierungen von Geräten, der Zugriff auf Daten und Applikationen nur innerhalb klar definierter, sicherer Rahmenbedingungen erfolgt. Dadurch wird eine Struktur erstellt, denn du aus deiner Sicht für dein Unternehmen als sicher einstuft.

Merke:

Erst wenn diese Basiskonfiguration in Entra ID sauber steht, solltest du mit der Verwaltung mobiler Geräte über Intune beginnen.

Das Vorgehen folgt dem Prinzip einer sogenannten **Tenant-Härtung**:

Eine strukturierte Absicherung und Konfiguration deines gesamten Microsoft Tenants mit besonderem Fokus auf Sicherheits- und Mobile-Device-Management.

Sobald die grundlegenden Sicherheits- und Compliance-Einstellungen stehen, gelangst du zu dem Bereich, in dem es um **Devices**, **Managed Devices**, **BOYD (Bring Your Own Device)** und **Device Risk** geht. In diesem Kontext sprechen wir dann über den **Endpoint Manager** respektive **Microsoft Intune** sowie über den **Defender for Endpoint**.

Ein wichtiger Punkt: **Defender for Endpoint** ist ausschließlich eine **Endpoint Protection-Lösung** – also ein Schutzmechanismus für Endgeräte gegen Bedrohungen wie Malware, Ransomware und andere Angriffe. Es handelt sich **nicht** um eine Mobile Device Management (MDM)-Lösung.

Wenn du die Verwaltung und Steuerung von mobilen Geräten oder Endpoints übernehmen möchtest, ist hierfür **Microsoft Intune** beziehungsweise der **Endpoint Manager** zuständig.

Wichtig zu wissen:

Du benötigst **Defender for Endpoint nicht**, um **Intune** oder den **Endpoint Manager** zu nutzen.

Und umgekehrt: Auch wenn deine Microsoft 365 Lizenz – etwa ab Business Premium – bereits eine Lizenz für Defender for Endpoint beinhaltet, bist du **nicht verpflichtet**, diese Lösung einzusetzen.

Wenn du bereits eine andere Endpoint-Security-Lösung im Einsatz hast, zum Beispiel eine Drittanbieter-Software, die sowohl Malware-Schutz als auch die Firewall auf den Endgeräten übernimmt, ist das vollkommen in Ordnung und kompatibel.

Microsoft hat hier jedoch einen besonderen Vorteil eingebaut:

Über die sogenannte **Interkonnektivität** können die einzelnen Microsoft-Services – also etwa Entra ID, Intune und Defender – miteinander kommunizieren, Signale austauschen und ihre Informationen kombinieren. Dadurch lassen sich Sicherheitsvorgänge effizienter automatisieren und auswerten. Diese tiefe Integration ist ein großer Pluspunkt der Microsoft-Cloud-Architektur.

Hier die Klarstellung:

Dienst	Aufgabe
Defender for Endpoint	Endpoint Protection Lösung (Schutz vor Malware, Exploits, Bedrohungen etc.)
Microsoft Intune	Vollumfängliches Mobile Device Management (MDM), Verwaltung von Geräten und Anwendungen

Tabelle 1: Vergleich Microsoft Intune vs. Defender for Endpoint

Sobald dein grundlegendes Mobile Device Management über Intune läuft, kannst du weitere Schutzmechanismen aktivieren:

- **Defender for Cloud Apps:**

Dient der Erkennung und Kontrolle von Schatten-IT. Du kannst darüber definieren, welche Cloud-Services und SaaS-Anwendungen in deinem Unternehmen erlaubt sind.

- **Information Protection:**

Umsetzung einer technischen **Datenklassifizierung** und Schutz sensibler Informationen.

Hinweis:

Über 90 % der Unternehmen in Deutschland haben zwar organisatorische Vorgaben zur Datenklassifizierung, aber keine technische Umsetzung. In der Praxis führen reine organisatorische Maßnahmen ohne technische Unterstützung selten zum gewünschten Sicherheitsniveau.

Der **Defender for Cloud Apps** bietet dir die Möglichkeit, genau zu steuern, **welche Applikationen, Services, Webseiten und SaaS-Dienste** von den verwalteten Endgeräten aus genutzt werden dürfen. Mit seiner Hilfe kannst du die Nutzung überwachen und bei Bedarf gezielt einschränken.

In der Praxis zeigt sich jedoch, dass es in den meisten Unternehmen **gar nicht wirklich bekannt** ist, **welche Services und Anwendungen** ihre Nutzer tatsächlich verwenden. Dieses fehlende Bewusstsein sorgt dafür, dass der Einsatz einer Lösung wie Defender for Cloud Apps besonders sinnvoll ist, um die Schatten-IT sichtbar zu machen und zu kontrollieren.

Wenn du spontan denkst: "Schatten-IT ist bei uns kein Thema", kann ich dir versichern – es ist immer ein Thema.

Die Frage ist nur, in welchem Ausmaß.

Thema	Details
Problem	Fehlende Transparenz über genutzte Dienste und Applikationen (Schatten-IT).
Lösung	Einsatz von Defender for Cloud Apps zur Überwachung und Einschränkung von Anwendungen.
Funktionen von Defender for Cloud Apps	- Erkennen genutzter Cloud-Services und SaaS-Anwendungen- Identifizieren von Sicherheitsrisiken- Erstellen und Durchsetzen von Richtlinien
Nutzen für das Unternehmen	- Schutz sensibler Daten- Verbesserung der Compliance- Gezieltes Management von Applikationen
Praxis-Tipp	Regelmäßige Überprüfung der Ergebnisse und Anpassung der Richtlinien basierend auf neuen Erkenntnissen.

Tabelle 2: Aufzeigen Schatten IT und Lösung

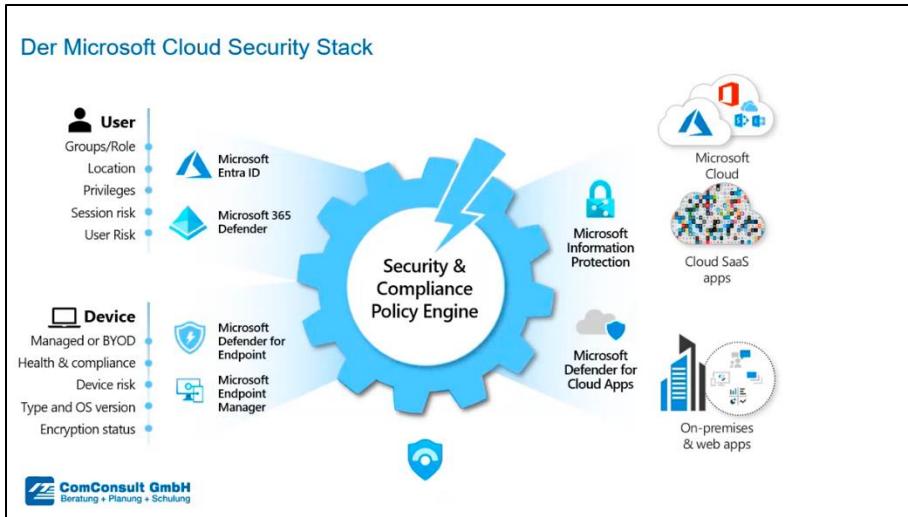


Bild 1: Microsoft Cloud Security Stack

Kapitel 2: Planung der Geräteverwaltung und Architekturentscheidung in Microsoft Intune

Bevor du dein Mobile Device Management (MDM) mit Microsoft Intune aufbaust, musst du dir eine zentrale Frage stellen: **Welche mobilen Endgeräte möchtest du überhaupt verwalten?**

Denn Microsoft Intune ist im Standardzustand so konfiguriert, dass **jede Plattform über jeden Registrierungsweg** erlaubt ist – mit einem **Limit von 15 Geräten pro Benutzer**. Ohne vorherige Planung blättert sich dein Asset-Park dadurch unnötig auf. Es besteht die Gefahr, dass sich Geräte in deiner Verwaltung wiederfinden, die du dort gar nicht haben möchtest.

Bevor du überhaupt beginnst, Geräte ins Intune zu übertragen, solltest du folgende Schritte durchführen:

- Definiere, **welche Gerätearten** (z. B. Windows, iOS, Android) du verwalten möchtest.
- Lege in den **Plattformeinschränkungen** und **Plattformlimits** die entsprechenden Werte fest.
- Entscheide, ob du beispielsweise neue Windows-11-Geräte bevorzugst oder noch Windows-10-Systeme verwalten möchtest.
- Bestimme, ob auch Apple-Geräte (iOS, iPadOS, macOS) sowie Android-Devices in den Verwaltungsumfang fallen sollen.
- Prüfe, ob du zusätzlich **Linux** oder **Chrome OS** Geräte zumindest in eine **Konformitätsüberwachung** aufnehmen möchtest (ohne vollständiges Management). Sprich nur die Überprüfung, ob das Gerät in eine Richtlinie reinfällt und diese auch einhält.

Hierbei solltest du auch berücksichtigen:

Bei Apple-Geräten gibt es erfahrungsgemäß weniger Herausforderungen bei der Registrierung.

Bei Windows- und Android-Geräten hingegen empfiehlt sich ein möglichst **homogenes Gerätelandschaftsmodell**.

Vermeide eine unnötige Gerätevielfalt wie zehn verschiedene Smartphone-Modelle und versuche, die Modellanzahl auf zwei bis drei Typen zu beschränken.

Das erleichtert nicht nur die **Registrierung und Fehlersuche**, sondern ermöglicht es dir auch, **schneller eine interne Knowledge Base** für bekannte Probleme aufzubauen.

Ein kleiner Praxis-Tipp:

Geräte im Budgetbereich von etwa **150 € oder niedriger** bei Android-Systemen können bereits bei der Registrierung und Umsetzung von Richtlinien spürbare **Performanceeinbußen** zeigen. Das stammt aus realen Projekterfahrungen, insbesondere im internationalen Umfeld.

Nachdem du die Entscheidung zur Gerätelandschaft getroffen hast, folgt die nächste Überlegung: **Wie soll die zentrale Verwaltung durchgeführt werden?**

Hier hast du verschiedene Optionen:

Verwaltungsmethode	Beschreibung
Endpoint Manager/Intune (Reine Cloud-Verwaltung)	Komplette Verwaltung aller Geräte über die Cloud. Betrifft Windows, iOS und Android gleichermaßen.
CO-Management	Kombination aus Microsoft Endpoint Manager (Intune) und dem System Center Configuration Manager (SCCM) . Applikationen kommen vom SCCM, Richtlinien vom Intune (oder umgekehrt).
Hybride Bereitstellung	Lokale Verwaltung über Active Directory (AD) mit Synchronisation ins

	Entra ID (ehemals Azure AD) und automatischer Registrierung ins Intune mittels Gruppenrichtlinien (GPOs).
Drittanbieteranbindung	Verwaltung über externe MDM-Systeme ohne vollständige Integration in Microsoft 365.

Tabelle 3: Verwaltungsmethoden

Ein paar wichtige Details dazu:

- **Reine Cloud-Verwaltung** mit Intune bedeutet, dass alle Richtlinien, Apps und Gerätesteuerungen direkt über die Cloud laufen.
- **CO-Management** funktioniert **nur mit dem Configuration Manager**. Kein anderes Tool bietet bisher eine vollständige Integration mit Intune.
- **Hybride Bereitstellung** erlaubt eine Kombination: Die Geräte bleiben Teil der lokalen Domäne, können aber gleichzeitig Intune-Policies beziehen. Standardmäßig bleibt hier **lokales Active Directory die führende Instanz** – allerdings kannst du die Priorisierung auch ändern, sodass Intune der neue Primärmanager wird.

Zusätzlich bietet Intune mittlerweile die Möglichkeit, **lokale GPOs** zu exportieren und als **Cloud-Richtlinien** zu importieren.

Das frühere Argument „In der Cloud habe ich nicht die gleiche Steuerungstiefe wie lokal“ zieht also heute nicht mehr.

Bei allen Ansätzen gilt:

Du musst dich strategisch entscheiden, ob deine Organisation langfristig eher **in Richtung reine Cloudverwaltung** strebt oder ob weiterhin eine **hybride Umgebung** bestehen bleiben soll.

Falls hybride Verwaltung nötig bleibt, etwa wegen lokaler Systeme oder Anwendungen, kannst du trotzdem die Cloud-Funktionalitäten von Intune gezielt nutzen, ohne auf GPOs vollständig verzichten zu müssen.

Zusammengefasst:

Vor dem operativen Start mit Intune solltest du exakt definieren:

- **Welche Geräte** möchtest du verwalten?
- **Wie** möchtest du diese Geräte verwalten (Cloud only, hybrid, CO-Management)?

- **Welche Plattform- und Registrierungsrichtlinien** setzt du, um dein Asset-Management klar zu regeln?

Onboarding und Szenarien - Ablösung und Integration

- ▣ **Welche** (mobilen) Endgeräte möchte ich in meine Verwaltung aufnehmen?

- ▣ Windows 10 / 11
- ▣ iOS / iPad OS / MacOS
- ▣ Android



- ▣ **Wie und womit** soll die **zentrale Verwaltung** durchgeführt werden?

- ▣ Endpoint Manager > Intune
- ▣ Co-Management in Richtung SCCM
- ▣ Hybride Bereitstellung
- ▣ Dritt-Anbieter Anbindung

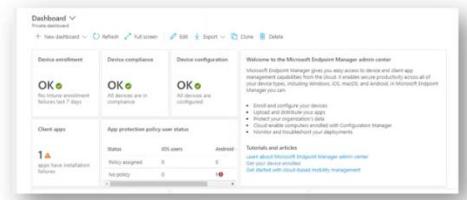


Bild 2: Onboarding und Szenario: Ablösung und Integration

Kapitel 3: Geräteszenarien und Registrierungswege in Microsoft Intune

Bevor du konkrete Schritte im Microsoft Intune unternimmst, musst du dich mit einer der zentralen Entscheidungen auseinandersetzen: **Welche Geräteszenarien möchtest du verwenden?**

Denn die Art und Weise, wie Geräte registriert werden, bestimmt maßgeblich, **welche Verwaltungsmöglichkeiten** du später auf diesen Geräten hast.

Das Thema betrifft besonders **iOS** und **Android**. Bei Windows ist der Einfluss zwar etwas geringer, dennoch ist die Auswahl der richtigen Registrierungsart ein **elementar wichtiger Schritt**.

Ein Gerät falsch zu registrieren und dann neu zu registrieren, bedeutet Aufwand – **und dieser Aufwand ist oft schmerhaft**. Deswegen solltest du dir von Anfang an ein klares Bild verschaffen, welche Szenarien für dein Unternehmen sinnvoll sind.

Übersicht über die Geräteszenarien

Hier eine kurze Zusammenfassung der gängigen Registrierungsmodelle:

- **Bring Your Own Device (BYOD)**

Der User bringt sein eigenes Gerät mit und dieses wird in die Verwaltung aufgenommen. Diese Geräte sind am einfachsten zu registrieren. Bei Android musst du die alte Geräteplattform des Android Device Administrators deaktivieren und entsprechend Android Enterprise aktiviert lassen. Momentan ist immer noch beides standardmäßig aktiv. Damit du nicht in die alte Verwaltungsplattform reinrutschst, solltest du die alte deaktivieren.

Wichtig: In der Realität ist BYOD selten wirklich freiwillig. Meistens handelt es sich eher um „This is your device“ und das darfst du privat mitnutzen.

- **Corporate-owned**

Geräte sind vollständig im Besitz des Unternehmens und dürfen **nur dienstlich** genutzt werden. Das sind also vollständig verwaltete Geräte.

- **Corporate-owned with work profiles**

Geräte gehören dem Unternehmen, dürfen aber **sowohl dienstlich als auch privat** genutzt werden. Datenbereiche werden strikt voneinander getrennt.

- **KIOSK-/Shared-Geräte**

Geräte, die **von mehreren Personen** genutzt werden, ohne dass sie eindeutig einem Benutzer zugeordnet sind.

Registrierungswege: Was musst du beachten?

Die Registrierungswege unterscheiden sich je nach Plattform:

- **Android**

BYOD-Geräte werden typischerweise direkt über die **Unternehmensportal-App** registriert. Für firmeneigene Geräte wird häufig ein **QR-Code** verwendet.

- **iOS**

Viele Unternehmen machen den Fehler, iOS-Geräte einfach über die Unternehmensportal-App zu registrieren.

Ergebnis: Das Gerät wird **immer** als **persönliches Gerät (BYOD)** kategorisiert. Auch wenn du im Intune später den Typ auf „Unternehmen“ änderst, bleibt die **eingeschränkte Verwaltung** bestehen, da keine technische Trennung zwischen persönlichen und geschäftlichen Daten möglich ist.

Wenn du ein iOS-Gerät im **Intune-Portal** die **Eigentümerschaft** von „persönlich“ auf „Unternehmen“ änderst, bewirkt das **nur eine Anpassung der Kategorisierung, nicht jedoch** eine Verbesserung der **Verwaltungsmöglichkeiten** oder eine **Separierung** von geschäftlichen und privaten Daten.

Um eine saubere Trennung und vollständige Verwaltung zu erreichen, musst du von Beginn an sogenannte **Registrierungsprofiltypen** verwenden.

Für den Nutzer selbst ändert sich durch die Nutzung eines anderen Registrierungsprofils visuell nichts.

Alternativ kannst du explizite **BYOD-Profile** verwenden

Willst du Geräte richtig als Unternehmensgeräte registrieren, empfiehlt sich die Nutzung des **Apple Business Managers**:

Dabei werden die Geräte mit einer **verwalteten Apple ID** (z. B. auf Unternehmensbasis) verbunden, während der User zusätzlich eine private Apple ID für persönliche Daten nutzen kann. So werden beide Bereiche sauber getrennt.

Ein wichtiger Hinweis:

Mit **iOS 18** wird die direkte Registrierung über die Unternehmensportal-App **abgekündigt** werden. Du solltest daher frühzeitig auf die neuen Registrierungsarten umsteigen.

Vorteil der neuen Registrierungsprofile:

Wenn ein Gerät falsch registriert wurde, musst du es **nicht zurücksetzen**, um es erneut korrekt zu registrieren.

Achtung:

Willst du ein Gerät nachträglich in den **Apple Business Manager** aufnehmen, ist ein vollständiger **Reset** des Gerätes zwingend erforderlich.

Wenn du bei Android hingegen ein Gerät als BYOD registrieren willst, musst du es nicht zurücksetzen. Bei den anderen Typen Corporate und Corporate work profiles, KIOSK oder Shared ist es wiederum erforderlich.

Aufwand und strategische Überlegungen

Gerade bei großen Gerätelparks kann die Neuregistrierung schnell zu einer **gewaltigen Herausforderung** werden:

Wenn du hunderte oder tausende Geräte zurücksetzen, Benutzer ansprechen, Backups erstellen und die Geräte erneut konfigurieren musst, bindet das erhebliche Ressourcen.

Daher entscheiden sich viele Unternehmen für einen **Mischbetrieb**:

Neugeräte ab einem bestimmten Stichtag werden sauber nach den neuen Vorgaben registriert. **Bestandsgeräte** verbleiben als BYOD-registrierte Geräte, da diese ohne großen Aufwand weiter genutzt werden können. Im Verhältnis zwischen Aufwand und Nutzen ist diese Lösung oft praktikabler.

Beachte dabei: Auf den BYOD-registrierten Geräten wirst du nicht die **volle Richtlinienkontrolle** haben.

Viele Sicherheitsfeatures (z. B. Trennung von geschäftlichen und privaten Daten) stehen dort nicht zur Verfügung.

Sobald ein Bestandsgerät sein Lebensende erreicht und ersetzt wird, kannst du den **richtigen Weg der Registrierung** einhalten und so nach und nach deine Gerätebasis konsolidieren.

Grundsätzlicher Hinweis

Die **Anzahl der Geräte** beeinflusst **nicht die Struktur oder Art der erforderlichen Registrierungsprozesse**.

Ob du 100 oder 100.000 Geräte registrierst: Die Konfigurationen, Profile und Vorgehensweisen bleiben identisch.

Einiger Unterschied ist der **Zeitfaktor** für die Umsetzung.

Deshalb ist es so wichtig, bereits vor der ersten Registrierung eine **klare Entscheidung** zu treffen, welches Gerätemodell und welchen Registrierungsweg du verwenden möchtest.

Onboarding und Szenarien - Gerätelpark

▢ Welche (**Geräte-)**Szenarien sollen in meinem Asset-Park verwaltet werden:

- ▢ Bring your own device (**BYOD**)?
- ▢ Corporate-owned?
- ▢ Corporate-owned with work profiles?
- ▢ KIOSK-/Shared-Geräte?

▢ Lifecycle von Bestandsgeräten:

- ▢ Austausch oder manuelle Registrierung?


 Personally-owned devices with work profile
 Manage personal enrollments with work profiles.


 Corporate-owned dedicated devices
 Manage device owner enrollments for kiosk and task devices.


 Corporate-owned devices with work profiles
 Manage enrollments for corporate devices with work profiles.

Bulk enrollment methods


 Apple Configurator
 Manage Apple Configurator enrollment


 Enrollment program tokens
 Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

Enrollment targeting


 Enrollment types (preview)
 Manage User Enrollment and Device Enrollment options

ComConsult GmbH
Beratung + Planung + Schulung
siller.consulting
INTELLIGENCE FOR IT

Bild 3: Onboarding und Szenarien, Geräteszenarien

Kapitel 4: Gerätbestand und Konformität – die Basis für eine saubere Verwaltung

Bevor du mit der Verwaltung deiner mobilen Endgeräte in Microsoft Intune startest, solltest du dir einen klaren Überblick über deinen aktuellen Gerätbestand verschaffen. In der Praxis ist es nämlich häufig so, dass viele Unternehmen gar nicht genau wissen, welche Geräte sie

tatsächlich im Einsatz haben. Gerade im Mittelstand oder bei kleineren Firmen gibt es oft keine vollständig gepflegten Asset-Listen. In Konzernen hingegen ist es üblicher, dass solche Informationen strukturiert vorliegen.

Ein wichtiger Punkt an dieser Stelle ist das Thema **Seriennummernpflege**. Wenn du die Seriennummern deiner Geräte sauber dokumentiert hast, etwa in einer Asset-Datenbank oder im E-Mail-System, dann hilft dir das erheblich weiter. Mit gepflegten Seriennummern kannst du später gezielt arbeiten, etwa beim Aufbau dynamischer Gerätegruppen oder beim Zuweisen spezifischer Konfigurationsprofile.

Solltest du aktuell noch keine strukturierte Asset-Datenbank haben, ist das kein Grund zur Sorge – es lässt sich trotzdem alles umsetzen. Aber: Wenn die Möglichkeit besteht, solltest du diese Informationen künftig erfassen und pflegen.

Neben dem Bestandsmanagement ist ein weiteres zentrales Thema die **Konformität**. Hier musst du für deine Umgebung festlegen, welche Kriterien ein Gerät erfüllen muss, um als **konform** zu gelten. Die Konformität spielt eine entscheidende Rolle für die Sicherheit deiner Umgebung mit **Conditional Access**.

Mit Conditional Access kannst du steuern, dass sensible Dienste wie **Mails, Teams** oder andere Microsoft 365 Anwendungen nur dann zugänglich sind, wenn ein Gerät als konform eingestuft wurde.

Dabei prüft Intune unter anderem folgende Kriterien:

- Ist eine Mindestbetriebssystemversion installiert?
- Wurde das Gerät jailbreakt oder gerootet?
- Besteht ein gewisses Threadlevel auf dem Gerät?

Erst wenn ein Gerät alle definierten Anforderungen erfüllt, wird ihm der Zugriff auf Unternehmensressourcen erlaubt. Werden diese Bedingungen nicht eingehalten, wird der Zugriff verweigert.

Ein weiterer wichtiger Punkt ist: **Nur verwaltete Geräte** können überhaupt in den Zustand der Konformität gelangen. Geräte, die nicht in Intune registriert und verwaltet werden, können niemals als konform gelten.

Das bedeutet, dass du auch über die Verwaltung in Intune steuerst, welche Geräte als vertrauenswürdig eingestuft werden und Zugang zu Unternehmensdaten erhalten.

Später im Verlauf werden wir uns im Detail anschauen, wie du Konformitätsrichtlinien aufbaust, welche Regeln sinnvoll sind und wie du diese praktisch in Intune umsetzt. Es ist entscheidend, diese Basis sauber zu gestalten, damit du eine sichere, funktionierende und gut kontrollierbare Geräteumgebung etablierst.

Onboarding und Szenarien - Gerätelpark

- ▣ Prüfung des ‚Bestands‘ und strategische Ausrichtung
- ▣ Festlegen der **Konformitäten**:
 - ▣ Was muss auf dem Endgerät konfiguriert werden?
 - ▣ Welche Use-Cases sollen unterstützt werden?
 - ▣ Wie soll der interne App-Store gepflegt werden?
 - ▣ Datenfluss- und Zugriffsteuerung



Bild 4: Onboarding und Szenarien, Konformitäten

Kapitel 5: App-Schutzrichtlinien als zusätzlicher Sicherheitslayer

Nachdem die grundlegenden Themen rund um Gerätemanagement und Konformität stimmen, kannst du darüber nachdenken, ob App-Schutzrichtlinien (engl. App Protection Policies) in deinem Unternehmen zum Einsatz kommen sollen. Dieser Schritt sollte allerdings erst dann in Betracht gezogen werden, wenn die grundlegenden Strukturen wie die Plattformgrenzen, die

Geräteverwaltung und die Konformitätsrichtlinien bereits stehen. App-Schutzrichtlinien sind ein fortgeschrittenes Sicherheitsinstrument und wirken ergänzend zu bestehenden Maßnahmen.

App-Schutzrichtlinien ermöglichen es dir, innerhalb bestimmter Anwendungen gezielt einen Schutzmechanismus aufzubauen. Konkret bedeutet das: Sobald sich ein Benutzer mit einer geschäftlichen Adresse, die eine gültige Microsoft 365-Lizenz besitzt, in einer App anmeldet, wird eine App-Schutzrichtlinie aktiv. Diese Richtlinie sorgt dafür, dass die betreffende App als **Managed App** behandelt wird.

Der Benutzer merkt davon zunächst wenig – im Hintergrund wird die App jedoch logisch in einen Container gepackt. Dieser Container ermöglicht es dir, verschiedene Schutzmechanismen zu aktivieren:

- Du kannst verhindern, dass Inhalte aus der App herauskopiert oder herausgeschnitten werden.
- Du kannst das Erstellen von Screenshots in der App unterbinden.
- Du kannst Funktionen wie „Senden an“ oder „Öffnen mit“ deaktivieren, um Daten innerhalb der App zu isolieren.

Das Ziel dabei ist, zu verhindern, dass sensible Unternehmensdaten unkontrolliert in nicht geschützte Bereiche des Geräts oder in andere Apps gelangen.

Ein weiterer wichtiger Aspekt ist, dass App-Schutzrichtlinien sowohl auf **verwalteten Geräten** als auch auf **nicht verwalteten Geräten** eingesetzt werden können. Dafür können Filter verwendet werden, die gezielt entscheiden, wann und auf welchen Gerätetypen die Richtlinien greifen.

Tendenziell haben sich zwei Nutzungsszenarien für App-Schutzrichtlinien etabliert:

App-Schutzrichtlinien auf verwalteten Geräten:

Hier dienen sie als zusätzlicher Schutzhierarchie auf ohnehin gemanagten Endgeräten. Selbst wenn ein Gerät kompromittiert wäre, könnten die Schutzmechanismen innerhalb der Apps weiterhin greifen und Unternehmensdaten schützen.

App-Schutzrichtlinien auf nicht verwalteten Geräten:

Gerade externe Dienstleister, Partner oder Consultants, die mit ihren privaten Smartphones arbeiten, können so sicher auf Unternehmensdaten zugreifen, ohne dass deren komplettes Gerät in die Verwaltung aufgenommen werden muss. Der Schutz bezieht sich ausschließlich auf die Unternehmensdaten innerhalb der jeweiligen App.

App-Schutzrichtlinien sind eine äußerst interessante und sinnvolle Erweiterung deines Mobile Device Managements – jedoch erst dann, wenn die Basis sauber aufgebaut ist.

Onboarding und Szenarien - Verwaltung von fremden Geräten

- ▶ **Nutzung von App-Schutzrichtlinien:**
 - ▢ Steuerung Datenfluss
 - ▢ Zusätzliche Zugriffsprüfung
- ▶ **Separierung der Geräte-Szenarien:**
 - ▢ Registrierte Geräte
 - ▢ Nicht-Registrierte Geräte
- ▶ **Validierung von externem Zugriff**

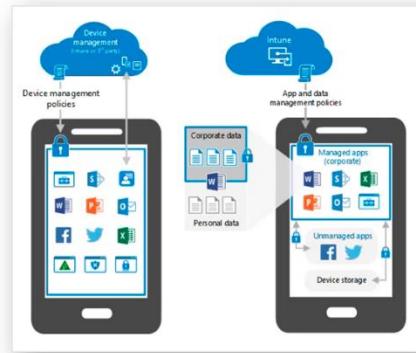


Bild 5: Onboarding und Szenarien, Verwaltung fremder Geräte

Kapitel 6: Erweiterung der lokalen Infrastruktur in Microsoft Intune

Ein weiterer zentraler Aspekt, ist die Erweiterung deiner lokalen Infrastruktur. Du hast zum Beispiel die Möglichkeit über Intune eine Verbindung zu einem lokalen File-Server aufzubauen. Du kannst aber auch deine bestehenden oder lokalen Gruppenrichtlinien validieren und entscheiden welche Intune sinnvoll direkt übernehmen kann. Direkte Übernahme heißt durch direkte **Konfigurationsprofile**.

Dabei empfiehlt sich ein klar strukturierter Vorgehensplan, der sich in drei Stufen gliedert:

1. Integrierte Konfigurationsprofile prüfen und nutzen

Der erste Schritt sollte sein, zu schauen, welche deiner bisherigen Richtlinien sich bereits direkt durch die integrierten Konfigurationsmöglichkeiten in Intune abbilden lassen. Das sind Richtlinien, die du innerhalb von Intune ganz einfach durch das Setzen von Häkchen, Ein- und Ausschalten oder durch einfache Auswahlfelder konfigurieren kannst.

2. Administrative Vorlagen einsetzen

Sollte eine bestimmte Richtlinie nicht über die integrierten Profile abbildbar sein, kannst du auf die sogenannten **Administrativen Vorlagen** zurückgreifen. Das sind die klassischen Gruppenrichtlinien.

3. OMA-URI Settings verwenden

Als letzte Option kannst du die **OMA-URI-Einstellungen** nutzen. OMA-URIs (Open Mobile Alliance Uniform Resource Identifier) und diese sind mit dem Registry-Key zu vergleichen.

Diese Reihenfolge stellt keine zwingende Vorgabe dar, sondern basiert auf bewährten Erfahrungswerten aus vielen Kundenprojekten. Das Ziel dieser Herangehensweise ist es, eine möglichst reibungslose Implementierung deiner Richtlinien zu erreichen, das Troubleshooting im Problemfall zu erleichtern und die zukünftige Administration so effizient und wartungsarm wie möglich zu gestalten.

Onboarding und Szenarien - Übernahme von Konfigurationen

☒ Erweiterung der **lokalen Infrastruktur**:

- ☒ Applikationen und Dienste mit lokaler Authentifizierung
- ☒ Zugriff z.B.: auf lokalen File Server

☒ Übernahme von **Gruppenrichtlinien**:

- ☒ Integrierte Konfigurationsprofile
- ☒ Administrative Vorlagen
- ☒ OMA-URI

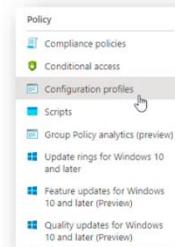


Bild 6: Onboarding und Szenarien, Übernahme Konfigurationen

Kapitel 7: Die verschiedenen Join-Typen in Entra ID und Intune

Bevor du deine Geräte zentral über Microsoft Intune verwalten kannst, solltest du unbedingt die verschiedenen Join-Typen kennen und verstehen. Sie sind entscheidend dafür, wie deine Endgeräte ins System aufgenommen werden, wie sie verwaltet werden können und welche Möglichkeiten sich im Anschluss durch die gewählte Methode ergeben.

Insgesamt unterscheidet Microsoft drei zentrale Join-Typen:

- Entra ID Registered (ehemals Azure AD Registered)
- Entra ID Joined
- Entra ID Hybrid Joined

Onboarding und Szenarien - Windows 10 & 11

Registrierungstyp	Registrierungsmethode	Gerät wird klassifiziert als...
Azure AD Registered	Office 365 Pro Plus / App mit geschäftlicher Mail-Adresse / Authentifizierung	Privates Gerät (BYOD!)
Azure AD Joined	Manueller Azure AD Join / AutoPilot	Unternehmensgerät
Hybrid Azure AD Joined	Lokale Gruppenrichtlinien / AutoPilot	Unternehmensgerät

Bild 7: Onboarding und Szenarien, Windows 10 & 11

Diese Typen unterscheiden sich deutlich voneinander – nicht nur in der technischen Umsetzung, sondern auch in ihrem Einsatzszenario. Beginnen wir mit dem komplexesten Modell:

Entra ID Hybrid Joined

Beim Entra ID Hybrid Join befindet sich das Computerkonto sowohl lokal im Active Directory als auch in der Cloud. Die Synchronisierung erfolgt über Entra ID Connect. Wenn du neue Geräte ausrollen willst, geschieht das typischerweise über den sogenannten AutoPilot Hybrid Join. Für Bestandsgeräte existiert eine passende Gruppenrichtlinie, die unter dem Namen MDMJoin bekannt ist.

Um den aktuellen Zustand eines Geräts zu prüfen, kannst du das Kommandozeilentool dsregcmd verwenden. Mit Befehlen wie /status, /join, /leave oder /force kannst du herausfinden, in welchem Zustand sich ein Gerät befindet. Wichtig: Die Anzeige erfolgt nicht immer sofort – es kann durchaus eine gewisse Zeit vergehen, bis ein erfolgreich synchronisiertes Gerät auch als „hybrid joined“ angezeigt wird.

Geräte, die über den Hybrid-Weg ins Intune aufgenommen werden, gelten aus Sicht von Intune als Unternehmensgeräte. Das bedeutet nicht zwingend, dass sie nicht auch privat genutzt werden können, aber in der Verwaltung gelten sie als Unternehmensgeräte.

Entra ID Joined

Ein weiterer Typ ist der Entra ID Join – auch bekannt als „Cloud Only“. Hierbei existiert das Computerkonto ausschließlich in Intune, es gibt also keine Verbindung zu einem lokalen AD mehr. Diese Art des Joinings eignet sich vor allem für Umgebungen, die vollständig cloudbasiert arbeiten oder dies zukünftig anstreben.

Auch bei Entra ID Join können Geräte über den AutoPilot registriert werden – in diesem Fall über den Autopilot Cloud Join. Alternativ gibt es auch die Möglichkeit, ein Gerät manuell zu registrieren. Dieser sogenannte manuelle Cloud Join wird über die Kontoeinstellungen in Windows durchgeführt, indem das Gerät mit einem Geschäfts- oder Schulkonto verbunden wird.

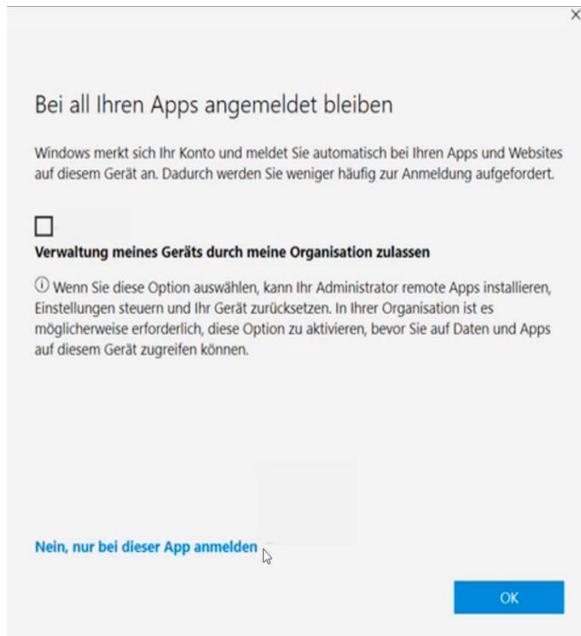
Diese manuelle Methode bietet sich in kleineren Infrastrukturen an – etwa wenn du nur über zehn bis zwanzig Geräte verfügst, die aktuell überhaupt nicht verwaltet werden. In solchen Fällen kann ein manueller Cloud Join eine pragmatische Lösung sein, um ohne Reinstallation oder komplexes Onboarding in Intune einzusteigen.

Auch bei Entra ID Joined gelten die Geräte in Intune als Unternehmensgeräte – unabhängig davon, dass sie „nur“ in der Cloud eingebunden sind.

Entra ID Registered

Dieser Typ wurde in diesem Abschnitt nur am Rande behandelt, spielt aber in der Praxis insbesondere bei BYOD-Szenarien (Bring Your Own Device) eine Rolle. Geräte, die Entra ID Registered sind, werden nicht vollständig vom Unternehmen verwaltet, sondern lediglich im Verzeichnis registriert. Diese Art der Einbindung dient häufig als Grundlage für

Appschutzrichtlinien oder minimale Compliance-Prüfungen, eignet sich aber nicht für eine tiefgehende Gerätekonfiguration.



Die sogenannten Entra ID Registered Geräte entstehen häufig über ein unscheinbares, aber folgenreiches Fenster in Windows. Viele IT-Fachkräfte und Nutzer kennen dieses Dialogfenster, in dem es heißt: „Verwaltung meines Geräts durch meine Organisation zulassen.“ Standardmäßig ist hier ein Haken gesetzt. In früheren Windows-Versionen – besonders vor Windows 11 – fehlte in diesem Fenster jeglicher erklärende Kontext.

Bild 8: Bei allen Apps angemeldet bleiben

Das führte dazu, dass sowohl Nutzer als auch Administratoren meist unbedacht auf „OK“ klickten. Wurde im Intune nichts hinterlegt, um dieses Verhalten zu unterbinden, registrierte sich das Gerät automatisch und erhielt den Status *Entra ID Registered*. Dabei spielt es keine Rolle, ob das Gerät zuvor bereits lokal eingebunden war oder nicht – die Registrierung erfolgt trotzdem. Später erkannte Microsoft das potenzielle Problem und ergänzte das Fenster um einen erläuternden Hinweistext. Dieser informiert nun darüber, dass durch Aktivierung der Option der Administrator unter anderem Apps installieren, Geräteeinstellungen verwalten und das Gerät sogar zurücksetzen kann. Die Registrierung in den Entra ID Registered Status kann damit gravierende administrative Auswirkungen haben – insbesondere dann, wenn sie unbeabsichtigt geschieht.

Leider hat der erklärende Hinweistext im Registrierungsfenster wenig Wirkung gezeigt – die meisten Benutzer klicken weiterhin reflexartig auf „OK“. Dabei wäre der korrekte Weg, um eine ungewollte Geräteeintragung zu vermeiden, unten links auf „Nein, nur bei dieser App anmelden“ zu klicken. In diesem Fall wird das Gerät nicht im Entra ID registriert, sondern lediglich eine Authentifizierung in der jeweiligen Applikation vorgenommen. Dieses Fenster erscheint typischerweise beim ersten Start von Microsoft 365-Anwendungen wie Teams,

Outlook oder Word, kann aber auch durch Drittanbieter-Apps ausgelöst werden, die eine Authentifizierung mit dem geschäftlichen Microsoft 365-Konto verlangen.

Das führt häufig dazu, dass private Geräte unbeabsichtigt im Entra ID – und manchmal sogar im Intune – registriert werden, sofern in den Organisationseinstellungen keine restriktiven Zugriffsregeln definiert wurden. Dieses Verhalten ist in vielen Unternehmen verbreitet, obwohl es nicht gewünscht ist. Microsoft hat in Windows 11 versucht, durch einen erweiterten Hinweistext mehr Bewusstsein für diese Situation zu schaffen, etwa mit Formulierungen wie „Ist das wirklich BYOD?“ – doch der Effekt bleibt begrenzt.

Ein technisches Detail ist dabei besonders wichtig: Das Fenster erscheint auch auf gemeinsam genutzten Geräten, etwa wenn sich mehrere Benutzer an einem einzigen Client anmelden. Ein Gerät kann sich mehrfach registrieren, jeweils mit einem unterschiedlichen primären Benutzer – dieser ist immer derjenige, der das Gerät zuerst registriert hat. Ob es sich dabei um eine oder zehn Personen handelt, ist für Entra ID und Intune unerheblich.

Geräte, die auf diese Weise registriert werden, gelten standardmäßig als *Entra ID Registered* und werden in Intune als *persönliches Eigentum* kategorisiert. Damit gelten sie technisch als BYOD-Geräte. In der Praxis zeigt sich, dass viele Unternehmen Geräte im Entra ID registered vorfinden, obwohl sie das gar nicht beabsichtigt haben.

Besonders verwirrend wird es durch ein Verhalten bei „Design“: Ein *Entra ID Hybrid Joined* Gerät kann zusätzlich als *Entra ID Registered* auftauchen – also mit zwei Kontotypen gleichzeitig. Microsoft beschreibt dieses Verhalten in offiziellen Learn-Artikeln, hat aber bislang keine vollständige Lösung gefunden. Es gibt Fälle, in denen dieses doppelte Konto angelegt wird, und andere, in denen das nicht geschieht. In Tech-Foren wie Reddit stößt dieses Verhalten regelmäßig auf Unverständnis. Microsoft ist sich dieses Verhaltens bewusst und hat mehrfach bestätigt, dass es keinen Schaden verursacht – aber eben auch keine konsistente Logik aufweist.

Ein Gerät, das *Hybrid Joined* ist, kann zusätzlich auch den Status *Registered* besitzen. Ist ein Gerät hingegen nur *Entra ID Registered*, dann hat es ausschließlich diesen Status. Wichtig ist dabei vor allem das Verständnis über die drei unterschiedlichen Join-Typen: *Entra ID Registered*, *Entra ID Joined* und *Entra ID Hybrid Joined*. Du solltest wissen, in welche Kategorien diese Geräte jeweils fallen und wie sie sich im Hinblick auf ihren Registrierungsweg unterscheiden – insbesondere in Bezug auf hybride Verwaltung und reine Cloud-Verwaltung.

Für die Verwaltung über Intune spielt es grundsätzlich keine Rolle, ob ein Gerät zuvor hybrid gejoined wurde oder nicht. Wenn es jedoch darum geht, zu verhindern, dass Unternehmensgeräte unbeabsichtigt, als *Entra ID Registered* registriert werden – etwa durch die bekannte Geräteanfrage in Windows – gibt es eine Einschränkung: Zwar erlaubt Intune, dass Windows-Geräte nicht als *Entra ID Registered* erfasst werden, jedoch ist dies in Entra ID selbst derzeit nicht mehr möglich. Eine entsprechende Einstellung, die es früher einmal gab, existiert aktuell nicht mehr.

Klar ist: Damit ein Gerät in Intune auftauchen kann, muss es zunächst im Entra ID registriert sein – der Join-Typ ist dabei zweitrangig. Umgekehrt gilt das jedoch nicht: Ein Gerät kann im Entra ID registriert sein, ohne jemals in Intune aufzutauchen.

Wenn du verhindern möchtest, dass das Registrierungsfenster auf Unternehmensgeräten erscheint, kannst du dies über einen Registry-Key steuern. Auf persönlichen Geräten lässt sich dieses Verhalten dagegen nicht unterbinden. An dieser Stelle kommt auch *Conditional Access* ins Spiel, mit dessen Hilfe du kontrollieren kannst, ob und unter welchen Bedingungen persönliche Geräte überhaupt registriert werden dürfen. Entscheidend ist, dass du diesen Zusammenhang verinnerlichst und verstehst, was hinter den Join-Typen und Registrierungsmechanismen steckt.

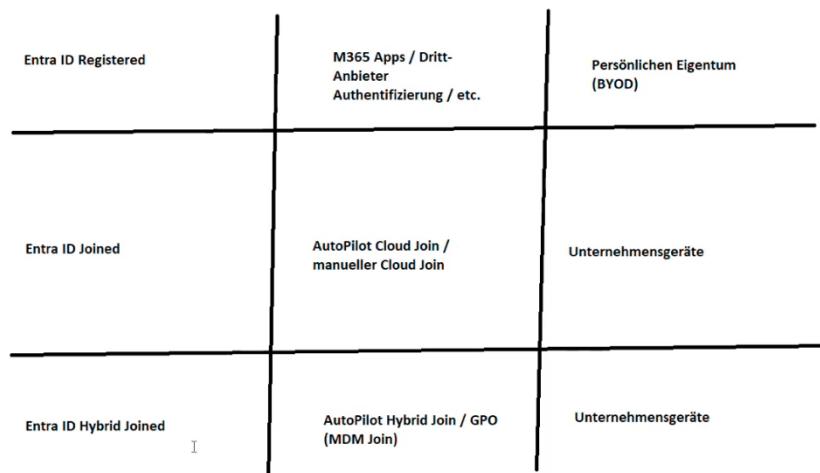


Bild 9: Registrierungstypen

Kapitel 8: Office-Installationen im Microsoft 365 Admin Center verwalten und ungewollte Geräte-Registrierungen in Entra ID vermeiden

Zunächst öffnest du das Microsoft 365 Admin Center. Navigiere dort zu den „Settings“. Innerhalb dieses Bereichs klickst du anschließend auf „Org Settings“ (Organisationseinstellungen). Achte darauf, dass du über die notwendigen administrativen Rechte verfügst – mindestens solltest du die Rolle des globalen Lesers haben. Falls dir entsprechende Rechte fehlen, kontaktiere deinen Administrator oder bitte darum, dir diese Rechte temporär zuzuweisen.

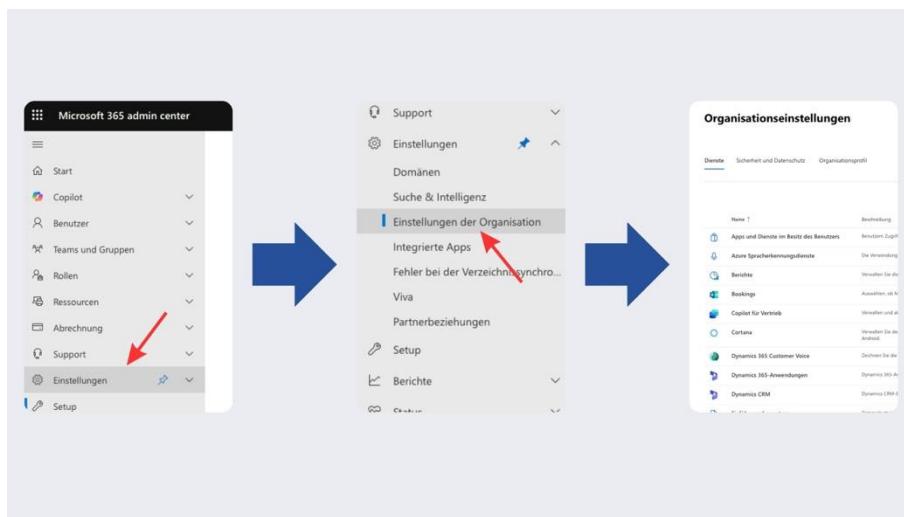


Bild 10: Organisationseinstellungen

Im Bereich der Organisationseinstellungen scrollst du dann nach unten zu den „**Microsoft 365 Installation Options**“. Klicke diesen Punkt an und gehe weiter zu „**Installation**“. Dort findest du die Option „Microsoft Apps: Users can install apps for Windows, mobile devices. Apps for Mac“ (sinngemäß: Benutzer dürfen Apps für Windows, Mobilgeräte oder Mac installieren). Je nach Lizenzierung kann es sein, dass du dort auch andere Applikationen wie angezeigt bekommst.

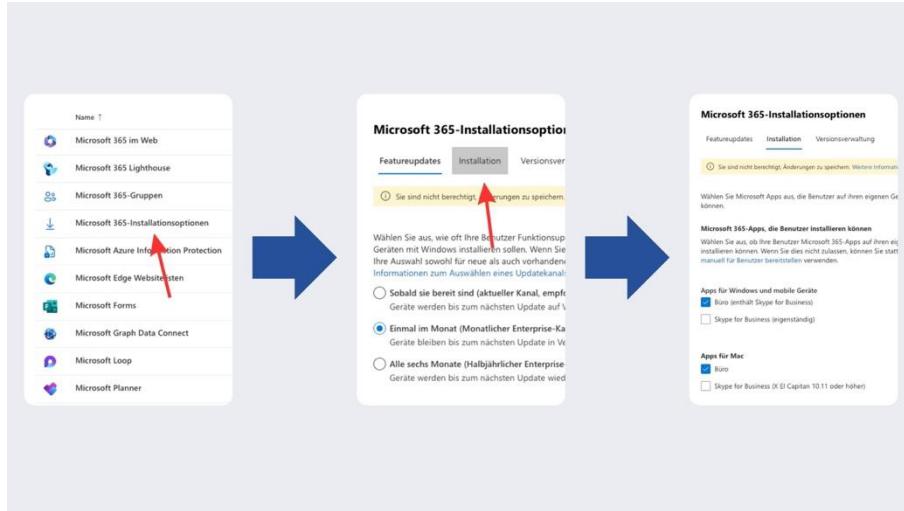


Bild 11: Was User installieren können

Hier ist der zentrale Punkt: Ist diese Option aktiviert, können Benutzer selbstständig auf office.com gehen, sich mit ihrem geschäftlichen Microsoft 365 Konto anmelden und die komplette Office Suite auf ihren privaten Geräten herunterladen und installieren. Dieser Prozess triggert in vielen Fällen das bekannte Registrierungsfenster für Entra ID, durch das sich ein Gerät automatisch in Entra ID registriert. Dies kann dazu führen, dass private Endgeräte in eurer Entra ID auftauchen – oft sogar im Intune – ohne dass ihr das als Organisation beabsichtigt habt.

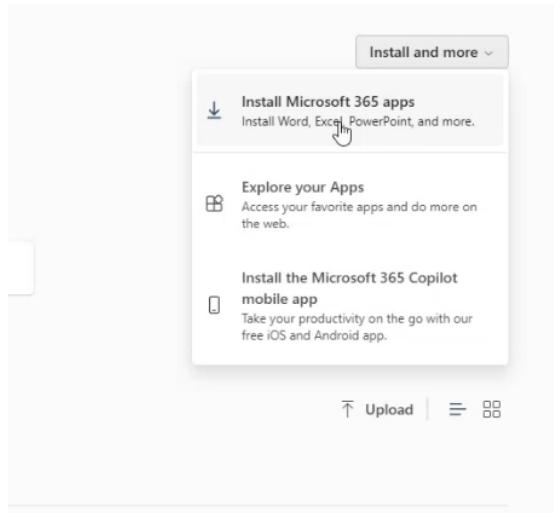


Bild 12: Installation Office Suite

Besonders kritisch wird dies, wenn Unternehmensdaten auf diesen nicht verwalteten, privaten Geräten landen. Auch Software-Installationen auf BYOD-Geräten (Bring Your Own Device)

können so ungewollt zustande kommen, möglicherweise in Kombination mit weiteren privaten Konten wie z. B. Gmail. Der technische Aufwand für diese Nutzeraktionen ist gering – das macht das Risiko umso größer.

Die Empfehlung lautet daher: Entscheide als Organisation zentral, wie und wann Office-Installationen bereitgestellt werden dürfen. Eine einfache Möglichkeit besteht darin, die besagte Option im Admin Center zu deaktivieren, indem du die Haken entfernst. Benötigt ein Benutzer zu einem bestimmten Zeitpunkt die Office Suite, kannst du den Haken temporär wieder setzen, die Installation durchführen und anschließend den Haken erneut entfernen. So minimierst du das Risiko unkontrollierter Installationen und der daraus resultierenden Registrierungen in Entra ID.

Nachverfolgung von Installationen

Zur Nachverfolgung von Office-Installationen existieren im Admin Center verschiedene Reporting-Funktionen. Gehe hierfür auf den Menüpunkt „**Reports**“ und wähle „**Usage**“ (Verwendung). Dort findest du z. B. den Report zu „**Microsoft 365 Apps**“, unter der wiederum der Abschnitt „**Activations**“ (Aktivierungen) angezeigt wird. Beachte jedoch: Diese Reports gelten nicht als besonders zuverlässig und sind in ihrer Aussagekraft eingeschränkt.

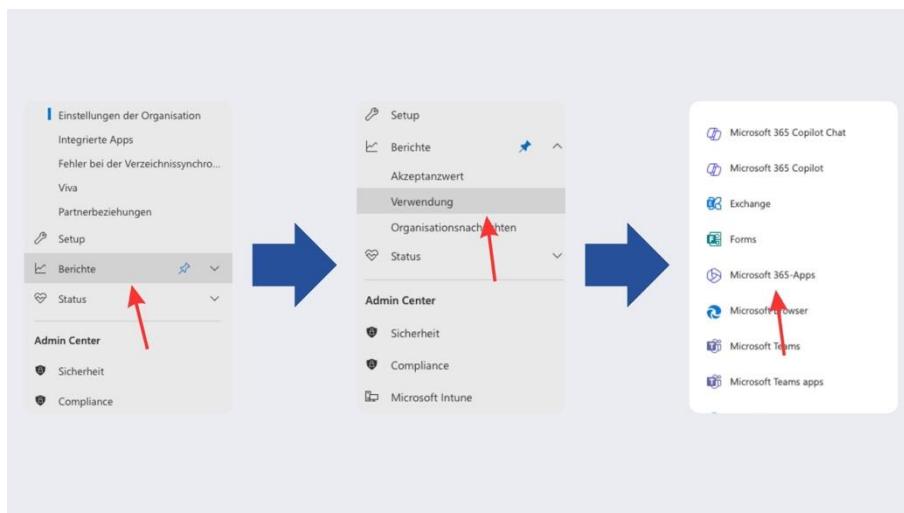


Bild 13: Nachverfolgung mit Reporting

Eine etwas genauere – wenn auch aufwendigere – Möglichkeit besteht darin, einzelne Benutzerprofile aufzurufen und dort im unteren Bereich die „**Microsoft 365 Activations**“ einzusehen. Klicke dafür auf „**View Microsoft 365 Activations**“. Auch diese Daten sind nicht vollständig fehlerfrei, liefern aber in der Praxis oft ein besseres Bild als die allgemeinen Aktivierungsreports.

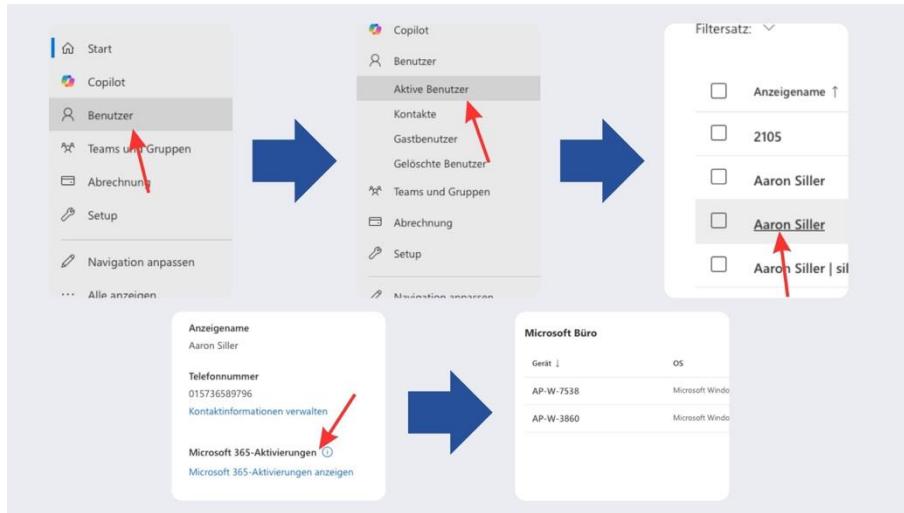


Bild 14: Über User nachverfolgen

Zugriff auf Drittanbieterspeicher in Microsoft 365 on the Web einschränken

Im Bereich „Org Settings“ findest du weiter unten die Option **Microsoft 365 on the Web**. Dort kannst du steuern, ob Benutzer innerhalb von Office Online (also z. B. Word oder Excel im Browser) Speicherorte von Drittanbietern einbinden dürfen.

Die Empfehlung lautet, diese Funktion zu deaktivieren. Damit verhinderst du, dass Benutzer ohne Rücksprache mit der IT eigene Speicherlösungen verwenden, die außerhalb der Compliance-Richtlinien der Organisation liegen. Stattdessen solltest du zentral festlegen, welche Speicherorte erlaubt sind – typischerweise **SharePoint**, **OneDrive for Business** und **Microsoft Teams**.

Praxisempfehlung:

Wenn eure Organisation alternative Speicherlösungen zulassen möchte, sollte dies bewusst durch die IT-Abteilung erfolgen – nicht durch einzelne Benutzer. Dies trägt zur Einheitlichkeit, Datenhoheit und Sicherheit bei.

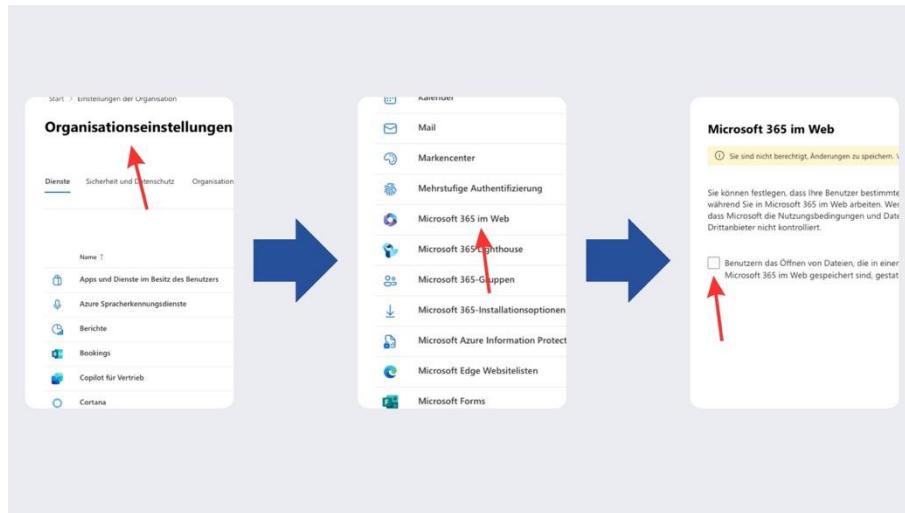


Bild 15: Microsoft im Web

Cortana-Zugriff auf M365-Daten einschränken

Ein weiterer Punkt betrifft **Cortana**, den digitalen Assistenten von Microsoft. Auch wenn Cortana nur in sehr spezifischen Szenarien eine Rolle spielt (z. B. in Windows 10 Version 1909 oder älter sowie in mobilen Apps), bietet das Admin Center hier eine zusätzliche Kontrollmöglichkeit.

Es empfiehlt sich, die Integration von Cortana mit Microsoft 365-Diensten ebenfalls zu deaktivieren. Dies ist keine klassische Sicherheitsmaßnahme, sondern dient der **Reduzierung von Metadaten**, wie sie etwa im Kontext der **DSGVO (Datenschutz-Grundverordnung)** relevant ist. Durch die Deaktivierung stellst du sicher, dass möglichst wenige personenbezogene Informationen über Spracheingaben oder Nutzerverhalten gesammelt und verarbeitet werden.

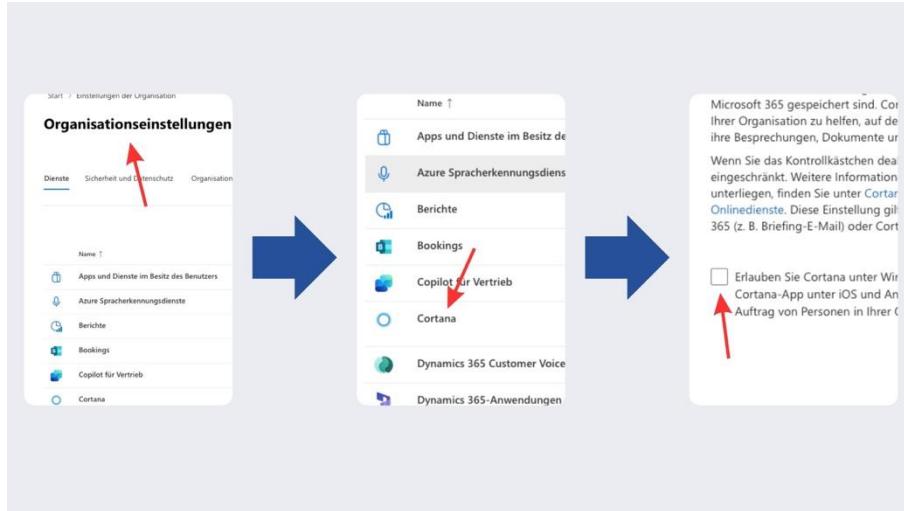


Bild 16: Cortana

Self Services für Benutzer deaktivieren

Ein besonders kritischer Bereich ist der Abschnitt **Self-service trials and purchases** im Admin Center. Hierunter fallen Funktionen und Lizenzmodelle, die Benutzer selbstständig aktivieren können – ohne Zutun der IT.

Im Standardzustand sind diese Funktionen **aktiviert**, was bedeutet, dass Benutzer beispielsweise kostenpflichtige Add-ons oder Testversionen eigenständig starten können. Dies kann sowohl zu **ungewollten Lizenzbuchungen** als auch zu **nicht genehmigter Nutzung von Cloud-Diensten** führen.

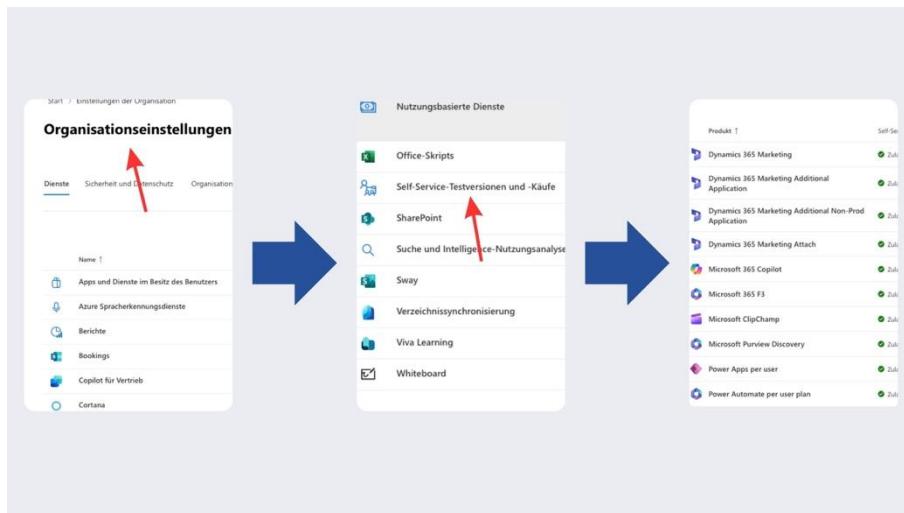


Bild 17: Self Service

Empfehlung für die Praxis:

Deaktiviere die Self Services zentral im Admin Center. Nur so behältst du als IT-Administrator den Überblick über die verwendeten Services und kannst sicherstellen, dass keine unerwünschten Kosten oder Sicherheitsrisiken entstehen.

Mit diesen Einstellungen stellst du sicher, dass zentrale Entscheidungen wie die Freigabe von Speicherorten, Diensten oder Zusatzfunktionen nicht dem einzelnen Benutzer überlassen werden. Das stärkt deine Rolle als Administrator und trägt zur Einhaltung von Sicherheits- und Compliance-Vorgaben in der Microsoft 365 Umgebung bei.

Wichtig zu wissen:

Microsoft ist bei diesem Thema inzwischen von einem **Opt-in-Modell** zu einem **Opt-out-Verhalten** übergegangen. Neue Self-Service-Möglichkeiten werden also automatisch aktiviert, sofern die Organisation sie nicht explizit **deaktiviert**. Solche Änderungen erfolgen oft ohne erkennbare Ankündigung – was das Risiko für ungeplante Zugriffe und IT-Schattenstrukturen zusätzlich erhöht.

Wähle einen Dienst aus und setze die Option auf „**Do not allow**“, um zu verhindern, dass Benutzer eigenständig Dienste aktivieren können.

Erfahren Sie, welche Produkte Self-Service-Testversionen anbieten

Zulassen

Benutzer können dieses Produkt selbst ausprobieren oder kaufen.

Nur Testversionen zulassen

Benutzer können dieses Produkt kostenlos testen, es aber nicht selbst kaufen. Wenn die Testversion endet, wird sie nicht in ein kostenpflichtiges Abonnement konvertiert, aber Benutzer können möglicherweise eine kostenpflichtige Lizenz von einem Administrator anfordern.

Nicht zulassen

Für dieses Produkt sind keine Self-Service-Käufe zulässig, in einigen Fällen sind jedoch möglicherweise noch kostenlose Testversionen verfügbar, und Benutzer können möglicherweise eine kostenpflichtige Lizenz von einem Administrator anfordern.

Bild 18: Nicht erlauben

Sollte tatsächlich Bedarf für ein Add-On oder eine Lizenz bestehen, kann der Zugriff gezielt und zeitlich begrenzt durch die IT-Abteilung gewährt werden. Zentralisierung ist hier das Stichwort – insbesondere im Hinblick auf **Sicherheit, Endgeräteverwaltung** und **Budgetkontrolle**.

Als nächstes gehst du im Microsoft 365 Admin Center in den Bereich **User owned Apps and Services** (bzw. „**Apps und Dienste im Besitz des Benutzers**“) und deaktiviere sowohl:

Office Store access/Office Store-Zugriff
Starting Trials/Testversionen

Sollte tatsächlich Bedarf für ein Add-On oder eine Lizenz bestehen, kann der Zugriff gezielt und zeitlich begrenzt durch die IT-Abteilung gewährt werden. Zentralisierung ist hier das Stichwort – insbesondere im Hinblick auf **Sicherheit, Endgeräteverwaltung** und **Budgetkontrolle**.

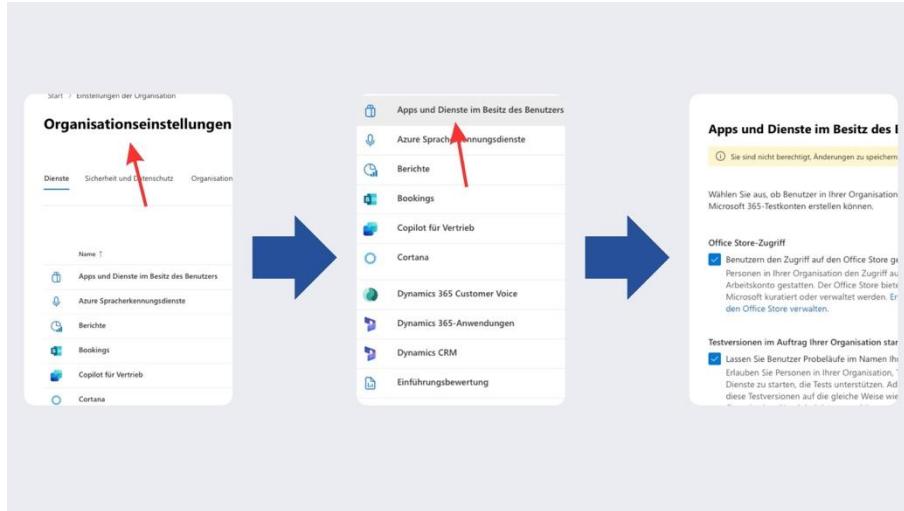


Bild 19: Apps und Dienste deaktivieren

Externer Zugriff auf SharePoint, OneDrive und Teams: Gastfreigaben sinnvoll konfigurieren

Ein weiterer Punkt im Kontext der Geräte- und Datenkontrolle ist der **externe Zugriff über SharePoint**. In den **SharePoint-Einstellungen** im **Microsoft 365 Admin Center** lässt sich festlegen, wie restriktiv externe Freigaben erfolgen dürfen.

Du findest dort vier Auswahlmöglichkeiten:

- Only people in your organization (nur interne Benutzer)
- Existing Guests only (nur bereits registrierte Gäste)
- New and Existing Guests (neue und bestehende Gäste)
- Anyone (jeder)

„**Only people in your organization**“ bedeutet, dass keinerlei Freigaben nach extern möglich sind – die Zusammenarbeit bleibt vollständig auf interne Benutzer beschränkt. Dieser restriktive Anwendungsfall kann jedoch im Laufe der Zeit durch eine aktiveren Nutzung von Teams, OneDrive oder SharePoint hinterfragt oder angepasst werden, sodass sich ein offeneres Freigabeszenario ergibt.

„**Existing guests only**“ bedeutet, dass die Freigabe von Inhalten nur an bereits in Entra ID registrierte Gastkonten erlaubt ist. Das bedeutet konkret: Möchte ein interner Benutzer z. B. eine Datei an eine externe Person – etwa Max Mustermann – freigeben, muss diese Person vorher manuell durch die IT als Gastbenutzer im Entra ID-Verzeichnis angelegt worden sein. Erst

nach Einladung und erfolgreicher Bestätigung kann der interne Benutzer mit Max Mustermann Inhalte teilen. Diese Vorgehensweise eignet sich insbesondere, wenn man einen kontrollierten Onboarding-Prozess für externe Partner etablieren möchte. Gleichzeitig stellt sich die Frage nach den vorhandenen Ressourcen: Wie häufig kommt so eine Anfrage vor – und wie oft möchte man diesen Prozess manuell durchführen?

„**New and existing guests**“ stellt einen pragmatischen Mittelweg dar: Hier können Benutzer auch selbst neue Gäste einladen, z. B. über die Teilen-Funktion in OneDrive, SharePoint oder Teams. Gibt ein Mitarbeiter die E-Mail-Adresse einer externen Person an, wird diese automatisch als Guest angelegt. Der eingeladene Benutzer muss sich über einen Einmalcode authentifizieren. Die IT-Abteilung erhält jedoch keine standardisierte Benachrichtigung darüber, von welchem Gerät und wann genau ein Shared Link freigegeben wurde – diese Nachverfolgbarkeit kann jedoch bei Bedarf konfiguriert werden.

Die Einstellung „**Anyone**“ erlaubt **anonyme Links** – also Freigaben ohne Authentifizierung. Das bedeutet: Eine Datei kann geteilt, weitergeleitet und von beliebigen Personen geöffnet werden, ohne dass du nachverfolgen kannst, wer darauf zugegriffen hat. Das stellt ein erhebliches Sicherheitsrisiko dar und sollte nach Möglichkeit **nicht verwendet werden**.

Empfohlene Praxis:

Setze die Freigabe-Einstellungen mindestens auf „**Existing Guests only**“ oder besser auf „**New and Existing Guests**“, je nach Organisationsgröße und Ressourcen.

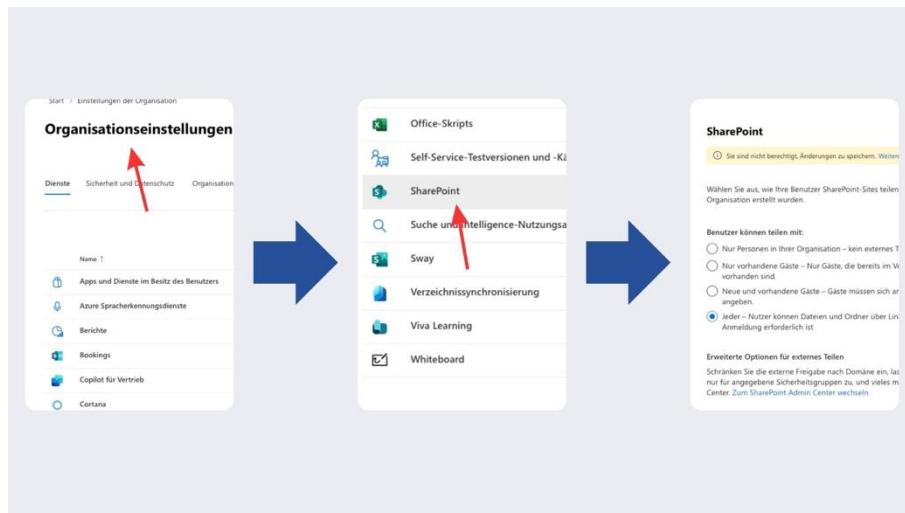


Bild 20: SharePoint

Vergleich der Freigabeoptionen für externe Benutzer in Microsoft 365

Option	Beschreibung	Sicherheitsniveau	Empfehlung
Anyone (Jeder)	Inhalte können per anonymer URL geteilt werden – ohne Anmeldung, komplett offen.	● Niedrig	Nicht empfohlen – keine Nachverfolgbarkeit, hohes Risiko bei Datenverlust.
New and Existing Guests	Benutzer dürfen neue externe Gäste selbst einladen. Authentifizierung über Einmalcode.	● Mittel	Flexibel, aber reduziert Kontrolle – sinnvoll bei ausreichenden Audit-Prozessen.
Existing Guests only	Nur Gäste, die zuvor durch die IT in Entra ID angelegt wurden, können Inhalte erhalten.	● Hoch	Empfohlen – gute Kontrolle, aber mehr Aufwand für die IT-Abteilung.
Only people in org.	Nur Personen aus der eigenen Organisation haben Zugriff. Keine externe Freigabe möglich.	● Sehr hoch	Maximale Sicherheit – sinnvoll bei stark regulierten Umgebungen.

Tabelle 4: Freigabeoptionen Vergleich

Hinweis zum Self-Service-Passwort-Reset

Ein zusätzlicher Punkt liegt im Bereich „**Security & Privacy**“ im Admin Center findest du den Eintrag „**Self-service password reset**“. Dieser verweist auf das Azure bzw. Entra ID Portal.

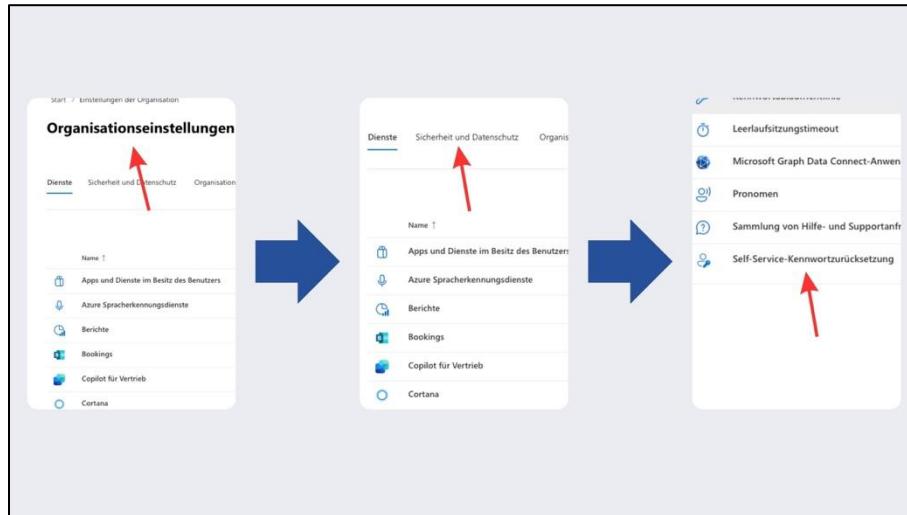


Bild 21:Self-Service password reset

Falls du den Self-Service Passwort-Reset aktivieren willst, klicke auf den Link „Go to the Azure Portal to turn on self-service password reset“. Dort kannst du im Entra ID Bereich diese Funktion zentral aktivieren und konfigurieren. Dieser Dienst ermöglicht es Benutzer*innen, ihr Kennwort

eigenständig zurückzusetzen, ohne den IT-Support kontaktieren zu müssen. Der Zugriff erfolgt über die Adresse aka.ms/sspr, welche bei Bedarf auch als benutzerfreundlichere URL maskiert werden kann.

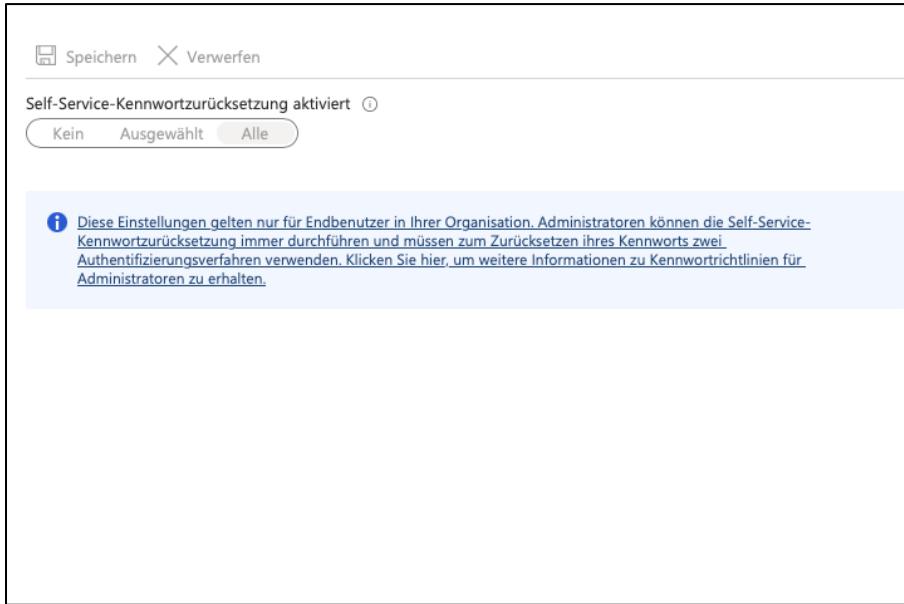


Bild 22: Self-Service password reset in Entra ID

Voraussetzung für die Nutzung ist, dass die Benutzer zuvor entsprechende Sicherheitsinformationen hinterlegt durch Sicherheitsfragen. Ziel ist es, den Helpdesk zu entlasten und den Supportaufwand bei klassischen Passwortverlusten zu reduzieren.

In der Praxis zeigt sich allerdings ein gemischtes Bild: Während einige Unternehmen positive Erfahrungen mit der Akzeptanz durch die Endanwender machen, nutzen andere den Dienst bislang nur testweise oder berichten von Nutzern, die sich trotz vorhandener Self-Service-Funktion weiterhin direkt an den IT-Support wenden.

Noch eine Information zur klassischen Passwortwechsel-Policy: In manchen Unternehmen besteht weiterhin die Vorgabe, Passwörter alle sechs Monate zu ändern. Diese Praxis gilt jedoch zunehmend als veraltet, da sie Anwender häufig dazu verleitet, einfache Muster zu verwenden (z. B. Hochzählen von Zahlen). Stattdessen wird heute empfohlen, auf **komplexe Passwörter mit mehr Zeichen** in Kombination mit **Multi-Faktor-Authentifizierung (MFA)** zu setzen.

Für Unternehmen, die eine Cyber-Versicherung anstreben, ist dies mittlerweile sogar häufig eine Grundvoraussetzung: Ein starkes Passwortkonzept in Verbindung mit MFA wird als zeitgemäßer und sicherer angesehen als regelmäßige Passwortänderungen allein.

Kapitel 9: Gastkonten, Benutzerrechte und Gruppenverwaltung in Microsoft Entra ID

Weiter geht es mit der Prüfung der Gastkonten im Mandanten. Gehe hierfür in deinem Microsoft Entra Admin Center zunächst in der linken Navigation auf „**Users**“ > „**All Users**“. Um herauszufinden, wie viele Gastbenutzer aktuell in deinem Mandanten existieren, nutze den „**Add Filter**“-Button, wähle als Filterkriterium „User type“ (im Deutschen: „Benutzertyp“) und setze den Operator-Wert auf „**Guest**“. So kannst du schnell validieren, ob und wie viele Gastkonten in deinem Verzeichnis vorhanden sind.

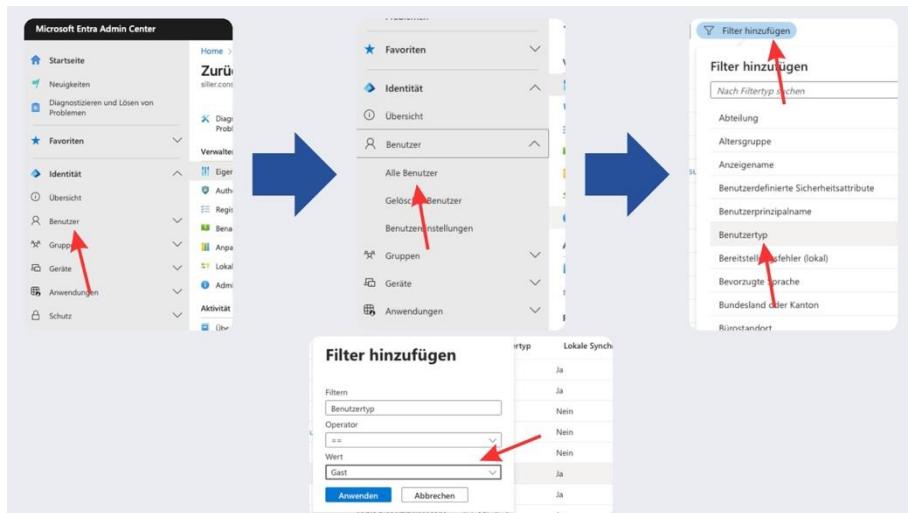


Bild 23: Gastkonten filtern

Wenn dabei keine Gäste angezeigt werden, ist das vollkommen in Ordnung – es hängt ganz von eurem Use Case ab. Vielleicht arbeitet ihr bisher rein intern ohne externen Zugriff. Wichtig ist allerdings der Hinweis: Sobald ein Benutzer in eurer Organisation über Tools wie Teams, SharePoint oder OneDrive mit einer externen Person interagiert (beispielsweise durch Teilen von Dateien), wird diese externe Person automatisch als Gastkonto im Verzeichnis angelegt.

Diese Gastkonten bleiben dauerhaft bestehen, es sei denn, du kümmert dich aktiv um deren Entfernung. Automatisiert funktioniert das nur mit sogenannten **Access Reviews**, die jedoch eine **Entra ID P2-Lizenz** erfordern. Alternativ kannst du per **PowerShell-Skript** eine Prüfung des „Last Login Date“ durchführen und Konten löschen, die beispielsweise seit mehr als sechs Monaten inaktiv sind.

Benutzerrechte unter „User Settings“

Wechsle nun im Menü zu „**User Settings**“. Hier findest du verschiedene sicherheitsrelevante Einstellungen, die du im Sinne der IT-Governance überprüfen solltest. Im Folgenden gehen wir auf die wichtigsten Optionen ein.

Die Option „**Users can register applications**“ erlaubt es Nutzern, über myaccount.microsoft.com selbstständig Applikationen im Entra ID zu registrieren. In der Praxis ist das meist unerwünscht, da Applikationen zentral bereitgestellt werden sollten. Empfehlung: **Schalte diese Option auf „No“**, um unkontrollierte App-Registrierungen zu vermeiden.

Mit der Einstellung „**Restrict non-admin users from creating tenants**“ kannst du verhindern, dass reguläre Benutzer eigenständig neue Mandanten anlegen. Zwar kann dies für Entwicklung oder Tests sinnvoll sein, sollte aber zentral gesteuert werden. Empfehlung: **Setze diesen Schalter auf „Yes“**, um spontane Mandantenerstellungen zu unterbinden.

Unternehmen sollten genau regeln, ob Benutzer **Security Groups** selbstständig erstellen dürfen. In den meisten Fällen ist das nicht notwendig – für die tägliche Arbeit reichen **Microsoft 365-Gruppen**, insbesondere im Zusammenhang mit Teams. Empfehlung: **Deaktiviere die Erstellung von Sicherheitsgruppen durch Nutzer**, also „**No**“.

In demselben Einstellungsbereich findest du Optionen zur Einschränkung des Gastzugriffs (**Guest user access restrictions**). Die sicherste Variante ist: „**Most restrictive**“.

Die drei Auswahloptionen bei den Gastzugriffsrechten steuern, in welchem Umfang Gäste andere Inhalte im Mandanten finden und durchsuchen können:

- Die **oberste Option** erlaubt es Gästen, über die **Enterprise Search** (z. B. in Teams oder SharePoint) nach beliebigen Objekten innerhalb des Mandanten zu suchen – auch außerhalb ihrer eigenen Gruppen oder Teams. Das stellt ein potenzielles Sicherheitsrisiko dar.
- Die **mittlere Option** beschränkt die Suche auf **jene Gruppen oder Instanzen, in denen der Gast explizit Mitglied ist**. Gäste sehen also nur Inhalte, auf die sie tatsächlich Zugriff haben.
- Die **unterste Option** ist die restaktivste: Gäste **dürfen überhaupt nicht suchen**. Sie können nur gezielt auf Inhalte zugreifen, die direkt mit ihnen geteilt wurden – etwa über einen Link. Das bietet die höchste Sicherheit und wird für die meisten Szenarien empfohlen.

Auch solltest du die Einstellung „**Restrict access to Microsoft Entra admin center**“ auf „**Yes**“ setzen. Der Zugriff auf das Entra Admin Center sollte ausschließlich Administratoren vorbehalten sein.

Ein weiterer Punkt betrifft **LinkedIn Account Connections**. Diese Verbindung erlaubt es Benutzern, ihre Geschäftskonten mit LinkedIn zu verknüpfen. Das ist datenschutztechnisch kritisch und kann dazu führen, dass Informationen aus dem Arbeitskontext in private Netzwerke gelangen. Empfehlung: **Setze diese Option auf „No“**. Wenn du diese Funktion einmal benötigst, kannst du sie temporär aktivieren.

Benutzer | Benutzereinstellungen

Alle Benutzer Überwachungsprotokolle Anmeldeprotokolle Diagnose und Problembearbeitung Gelöschte Benutzer Kennwortrücksetzung Benutzereinstellungen Ergebnisse von Massenvorgängen Neue Supportanfrage

Aktualisieren | Haben Sie Feedback?

Standardberechtigungen für Benutzerrollen

Weitere Informationen

Benutzer können Anwendungen registrieren Nein
Benutzer ohne Administratorrechte daran hindern, Mandanten zu erstellen Ja
Benutzer können Sicherheitsgruppen erstellen Nein

Gastbenutzerzugriff

Weitere Informationen

Zugriffsbeschränkungen für Gastbenutzer
 Gastbenutzer haben denselben Zugriff wie Mitglieder (um Gastbenutzer haben eingeschränkten Zugriff auf Eigenschaften und Mitglieder zu verhindern)
 Der Gastbenutzerzugriff ist auf Eigenschaften und Mitglieder beschränkt

Verwaltungszentrum

Weitere Informationen

Zugriff auf Microsoft Entra Admin Center einschränken Ja

LinkedIn-Kontoverbindungen

Weitere Informationen

Gestatten Sie Benutzern, ihr Geschäfts-, Schul- oder Unikonto mit LinkedIn zu verbinden. Ja
 Ausgewählte Gruppe
 Nein

Bild 24: Benutzereinstellungen

Steuerung der Gruppenanlage

Wenn du kontrollieren willst, welche Gruppen Benutzer erstellen, dürfen, gehe in den Bereich „General“. Dort findest du zwei relevante Optionen:

- Security Groups
- Microsoft 365 Groups

Beide sollten standardmäßig deaktiviert sein. Microsoft 365-Gruppen entstehen automatisch, wenn Benutzer ein neues Team in Microsoft Teams erstellen. Deshalb braucht es in der Regel keine manuelle Gruppenanlage durch die Nutzer.

Viele Nutzer wissen nicht, dass sie Microsoft 365-Gruppen auch unabhängig von Teams anlegen können – was aber selten notwendig ist. Durch die Deaktivierung vermeidest du Wildwuchs und behältst die Kontrolle über die Gruppenlandschaft.

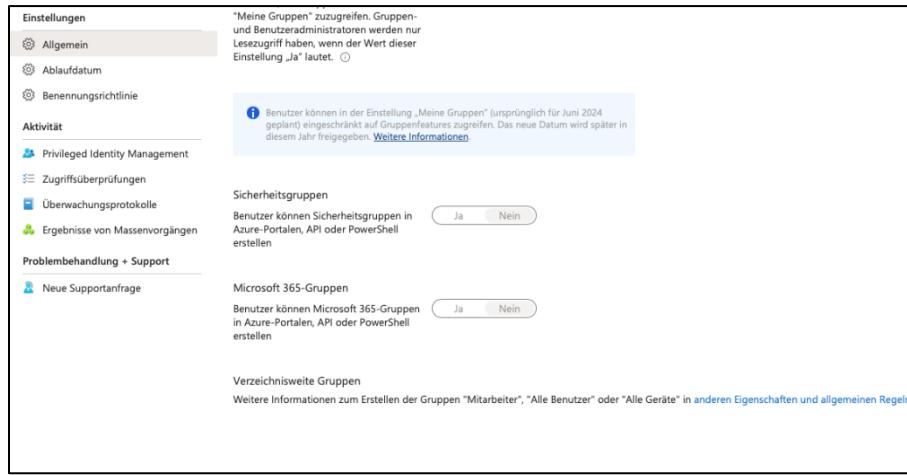
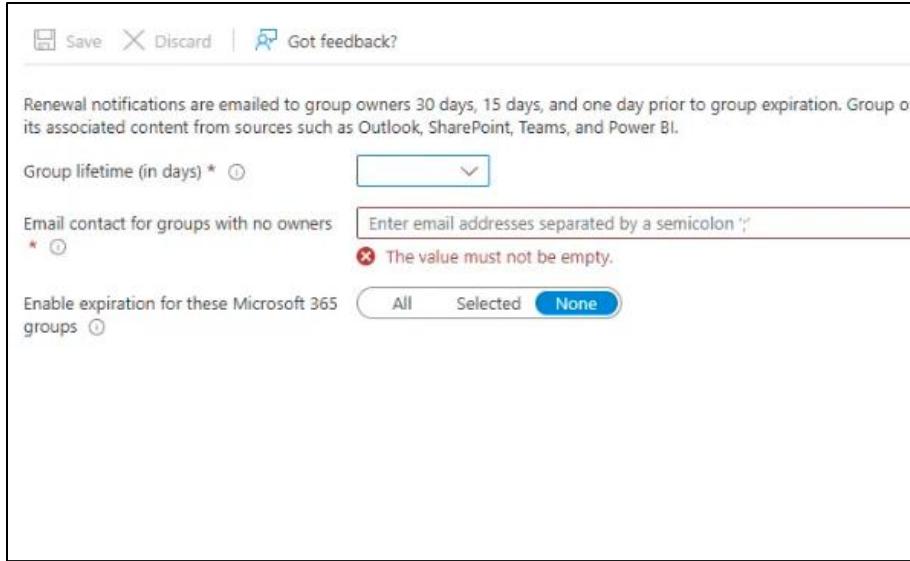


Bild 25: Microsoft 365 Gruppen anlegen

Ablaufdatum für Microsoft 365-Gruppen

Ein weiterer wichtiger Punkt betrifft die **Ablaufsteuerung von Gruppen**. Navigiere zu „Expiration“, um zu prüfen, ob hier bereits etwas konfiguriert wurde. Standardmäßig haben Microsoft 365-Gruppen kein Ablaufdatum. Das führt langfristig zu einer Vielzahl inaktiver oder veralteter Gruppen – insbesondere, wenn Teams nur für Testzwecke oder kurzfristige Projekte genutzt wurden.



The screenshot shows a configuration interface for Microsoft Groups. At the top, there are buttons for 'Save' and 'Discard', and a link 'Got feedback?'. Below this, a note states: 'Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners receive renewal notifications for their associated content from sources such as Outlook, SharePoint, Teams, and Power BI.' There are three main configuration sections:

- Group lifetime (in days) ***: A dropdown menu currently set to '365'.
- Email contact for groups with no owners ***: An input field containing 'Enter email addresses separated by a semicolon ;'. A validation error message 'The value must not be empty.' is displayed next to it.
- Enable expiration for these Microsoft 365 groups**: A button group with three options: 'All' (grayed out), 'Selected' (highlighted in blue), and 'None' (selected).

Bild 26: Ablaufdatum Gruppen

Microsoft Teams-Gruppen greifen dabei auf **unternehmensweite Ressourcen** zu. Zum Beispiel verfügt dein Mandat bei SharePoint standardmäßig über **1 TB Speicherplatz pro Tenant plus 10 GB pro lizenziertem Benutzer**. Jedes neue Teams reduziert also eure Speicherreserven.

Empfehlung: Konfiguriere eine „**Group Lifetime**“ von z. B. **365 Tagen**. Wenn innerhalb dieses Zeitraums keine Aktivität in einer Gruppe stattfindet – keine Chats, keine Dateiänderungen, keine Mitgliederänderungen – wird das Team zur Löschung markiert. Die Besitzer erhalten dann 30, 15 und 1 Tag vor Ablauf eine Benachrichtigung.

Wichtig: Sollte eine Gruppe **keinen Besitzer** haben (was in der Praxis vorkommen kann), richte am besten ein **zentrales Sammelpostfach** ein, über das du als Administrator informiert wirst. So vermeidest du unkontrollierte Gruppenlöschungen.

Beachte: Die Ablaufregel gilt **nicht rückwirkend**. Sie wird erst ab dem Zeitpunkt aktiv, an dem du sie konfigurierst.

Kapitel 10: Geräteeinstellungen und -registrierung in Microsoft Entra ID

Beginne im Microsoft Entra Admin Center unter dem Menüpunkt „**Devices**“ und wähle dort die Übersicht (**Overview**) aus. Im ersten Schritt solltest du prüfen, wie viele Geräte derzeit im Mandanten registriert sind. Diese Zahl kann ein Indikator für die aktuelle Konfiguration sein. Notiere dir die *Total Number of Devices* und überlege, ob sie der erwarteten Anzahl entspricht.

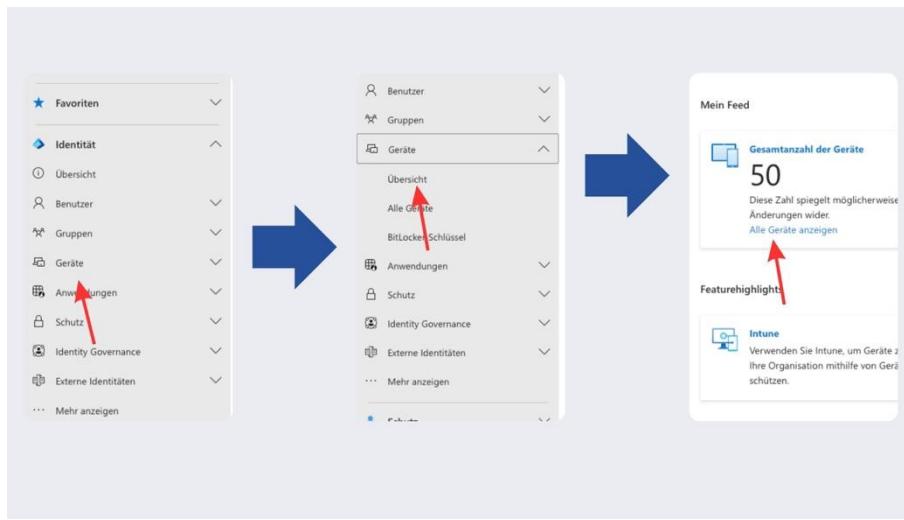


Bild 27: Gesamtzahl der Geräte

Gerade bei größeren Umgebungen ist es nicht unüblich, dass eine Vielzahl veralteter (stale) Geräte vorhanden ist – Geräte, die schon lange nicht mehr verwendet, aber nie entfernt wurden. Es lohnt sich hier, regelmäßig aufzuräumen und die Geräteliste zu pflegen, um einen besseren Überblick über den tatsächlichen Bestand zu erhalten.

Klicke im nächsten Schritt im Menü auf „**Device Settings**“. Hier findest du einige wichtige Konfigurationsmöglichkeiten, die du als Administrator verstehen und bewerten solltest.

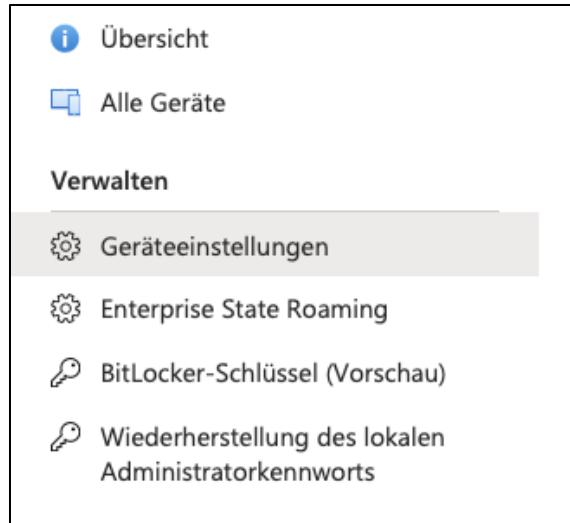


Bild 28: Geräteeinstellungen

Benutzer können Geräte mit Microsoft 365 verknüpfen

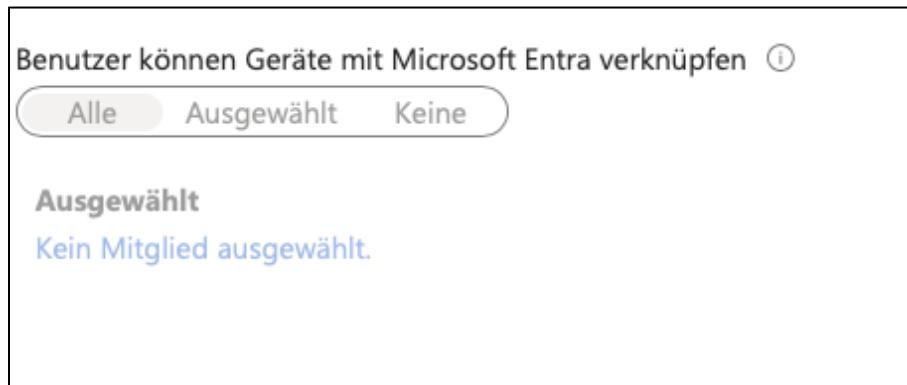


Bild 29: Geräte mit Microsoft Entra verknüpfen

Diese Einstellung erlaubt es Benutzern, Geräte direkt mit der Microsoft 365-Umgebung zu verbinden – also via **Microsoft Entra Join**, insbesondere in Verbindung mit Windows- oder macOS-Geräten. Sie gilt nicht für Hybrid Joins, Android-Geräte oder Autopilot Self-Deployment.

Wenn du auf das Informationssymbol neben der Option klickst, erhältst du eine englische Beschreibung, die diesen Geltungsbereich nochmals klarstellt.

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.

Bild 30: Hinweistext

Diese Option entscheidet also, ob und welche Benutzer ihre Geräte manuell oder per Autopilot in die Cloud-Umgebung aufnehmen dürfen. Wenn du beispielsweise planst, Autopilot für künftige Deployments zu nutzen, kann es sinnvoll sein, diese Option für einen bestimmten Benutzerkreis zu aktivieren. Falls jedoch keine Notwendigkeit besteht, solltest du die Funktion deaktivieren oder stark einschränken, um unbeabsichtigte Geräteverknüpfungen zu vermeiden.

Benutzer können ihre Geräte bei Microsoft Entra registrieren

Benutzer können ihre Geräte bei Microsoft Entra registrieren. ⓘ

Alle Keine

 [Weitere Informationen zur Funktionsweise dieser Einstellung](#)

Bild 31: Geräte bei Microsoft Entra registrieren

Diese Einstellung ist in den meisten Umgebungen **ausgegraut** – vermutlich auch bei dir. Das liegt daran, dass Microsoft diese Funktion in Umgebungen mit Intune-Lizenz entfernt und in **Microsoft Intune** selbst verschoben hat.

Früher konntest du hier direkt im Entra Admin Center festlegen, ob Benutzer Geräte zur Entra ID registrieren dürfen. Heute steuerst du das über **Geräteplattform-Einschränkungen in Intune**. Auch wenn es technische Workarounds (z. B. über PowerShell) gibt, um diese Einstellung wieder sichtbar zu machen, ist davon in produktiven Umgebungen eher abzuraten. Denn eine Rückkehr zur lokalen Steuerung bedeutet in der Praxis, dass alle bereits registrierten Geräte neu

aufgenommen werden müssten – ein Szenario, das nur bei **frischen oder vollständig neu aufgebauten Tenants** praktikabel ist.

Multi-Faktor-Authentifizierung für Registrierung oder Join erforderlich

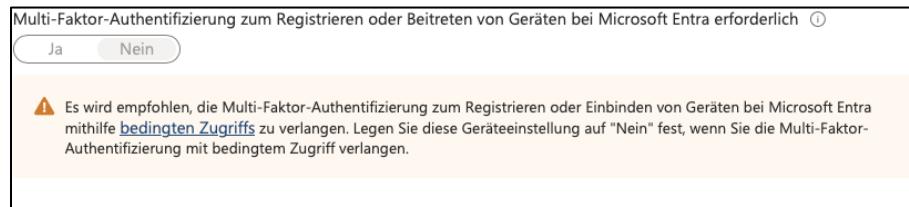


Bild 32: MFA für Registrierung

Diese Einstellung solltest du bewusst auf „**Nein**“ lassen. Denn auch wenn die Aktivierung der MFA hier theoretisch eine zusätzliche Hürde darstellt, empfiehlt Microsoft, das Thema **über Conditional Access zu regeln**.

Der Grund: Diese Option verhindert nicht zuverlässig, dass Geräte registriert werden – weder gewollt noch ungewollt. Es kann durchaus vorkommen, dass sich ein Gerät aus Versehen registriert, etwa durch eine unbeabsichtigte Benutzeraktion. Über Conditional Access Policies kannst du hingegen gezielt MFA bei bestimmten Aktionen oder Gerätekonfigurationen erzwingen. Das erhöht die Sicherheit und Awareness – beispielsweise, wenn ein Mitarbeiter plötzlich einen Anmeldehinweis bekommt, der auf eine neue Gerätekonfiguration hinweist. Solche Hinweise führen oft dazu, dass Rückfragen gestellt oder Vorfälle frühzeitig erkannt werden.

Gerätegrenzwerte, lokale Administratorrechte und Geräterezearchen

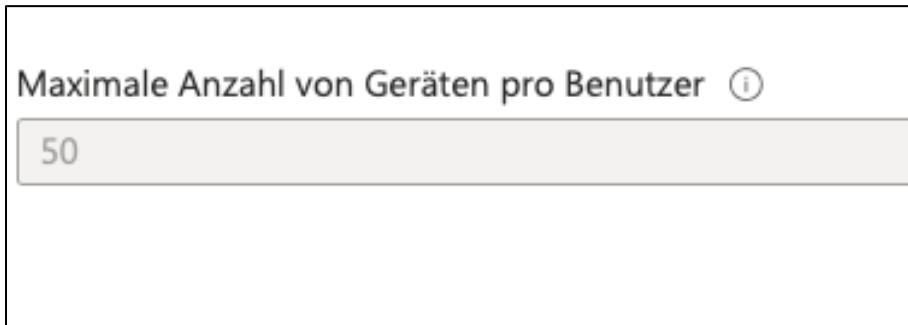


Bild 33: Maximale Anzahl Geräte

Ein weiterer Punkt, den du in der Gerätekonfiguration von Microsoft Entra ID beachten solltest, ist die maximale Anzahl der Geräte pro Benutzer. Diese Einstellung findest du ebenfalls unter **Microsoft Entra ID > Geräte > Geräteinstellungen**. Hier legst du fest, wie viele Geräte ein Benutzer maximal mit der Entra ID verbinden darf. Standardmäßig ist der Wert häufig auf 50 gesetzt, was früher sogar als empfohlener Wert galt. Inzwischen wird oft 20 vorgeschlagen – beide Werte sind jedoch deutlich überdimensioniert für typische Nutzungsszenarien.

Realistisch betrachtet, nutzen die meisten deiner User ein bis drei Geräte: z. B. ein Laptop, ein Smartphone und eventuell ein Tablet oder ein zweiter Client. Selbst fünf Geräte sind in den meisten Fällen bereits die Obergrenze. Deshalb solltest du diese Zahl bewusst heruntersetzen. Du kannst hierzu einfach den passenden Wert auswählen oder über die benutzerdefinierte Eingabe direkt eine Zahl wie **5** oder **3** wählen.

Wichtig ist dabei: Diese Einstellung wirkt sich **nicht** rückwirkend aus. Wenn ein Benutzer bereits beispielsweise acht Geräte registriert hat und du die Grenze im Nachhinein auf fünf setzt, bleiben die bestehenden Geräte weiterhin registriert. Es wird lediglich verhindert, dass zusätzliche Geräte hinzugefügt werden. In der Praxis bedeutet das: Wenn sich ein User beschwert, dass er beim Gerätekonfigurationsversuch eine Fehlermeldung erhält, liegt das vermutlich an diesem Grenzwert.

Tipp aus der Praxis: Ein häufiges Setup ist die Kombination aus **Laptop und Smartphone** – mehr benötigen viele Nutzer nicht. Setze den Grenzwert also ruhig bewusst konservativ. So behältst du Kontrolle über die Gerätelandschaft und minimierst ungewollte Registrierungen.

Umgang mit lokalen Administratorrechten

Ein besonders sicherheitsrelevanter Bereich in der Entra-Gerätekonfiguration betrifft die **lokalen Administratorrechte auf den Geräten**. Du solltest dir genau anschauen, wer bei euch aktuell lokale Adminrechte auf Clients besitzt und wie diese vergeben werden. Viele Organisationen verwenden mittlerweile **Microsoft LAPS (Local Administrator Password Solution)** – entweder lokal oder über Microsoft Intune – zur sicheren Verwaltung lokaler Adminkonten.

Früher war es üblich, dass der registrierende Benutzer automatisch beim Geräteeintritt lokale Administratorrechte erhielt. Falls diese Optionen bei dir noch aktiviert sind, **deaktiviere sie dringend**.

Es gibt zwei Einstellungen, auf die du achten solltest:

- Globale Administratoren erhalten lokale Adminrechte beim Entra Join
- Registrierende Benutzer erhalten lokale Adminrechte beim Entra Join

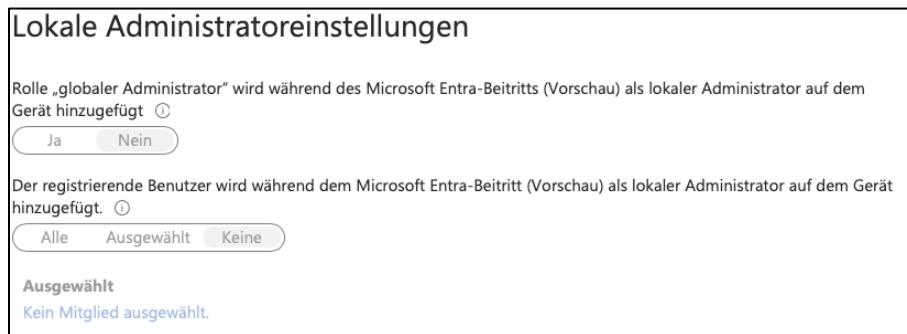


Bild 34: Lokale Administratoreinstellungen

Beide Optionen solltest du konsequent auf „**Nein**“ bzw. „**Keine**“ setzen. Der Hintergrund ist einfach: Wenn ein globaler Administrator kompromittiert wird, sind **alle** mit seinem Konto verbundenen Geräte potenziell gefährdet – ein enormes Sicherheitsrisiko. Auch der registrierende Benutzer sollte **nicht automatisch Adminrechte** erhalten. Wenn bestimmte Personen – etwa Entwickler – dennoch temporär lokale Adminrechte benötigen, gibt es Tools wie **Make Me Admin**, mit denen sich diese Rechte zeitlich begrenzt und kontrolliert gewähren lassen.

Falls du Microsoft LAPS über Intune verwendest, kannst du die entsprechende Option auf „Ja“ setzen. Das ermöglicht die sichere Verwaltung lokaler Adminkonten auf moderne Weise – inklusive automatisierter Passwortrotation und Zugriffskontrolle.

Validierung von registrierten Geräten

Ein sehr hilfreicher Schritt im Rahmen deiner Analyse ist die Überprüfung, **welche Geräte aktuell mit Microsoft Entra ID registriert** sind – insbesondere, ob sich dort **unerwartete Geräte** finden. Das betrifft insbesondere persönliche Geräte oder veraltete Einträge, etwa von Terminalservern, die mehrfach erscheinen.

Um diese Analyse durchzuführen, gehe wie folgt vor:

1. Navigiere zu Microsoft Entra ID > Geräte > Alle Geräte
2. Klicke auf Filter hinzufügen
3. Wähle den Filtertyp Verknüpfungstyp (Join Type) aus
4. Setze den Wert auf „Microsoft Entra registered“

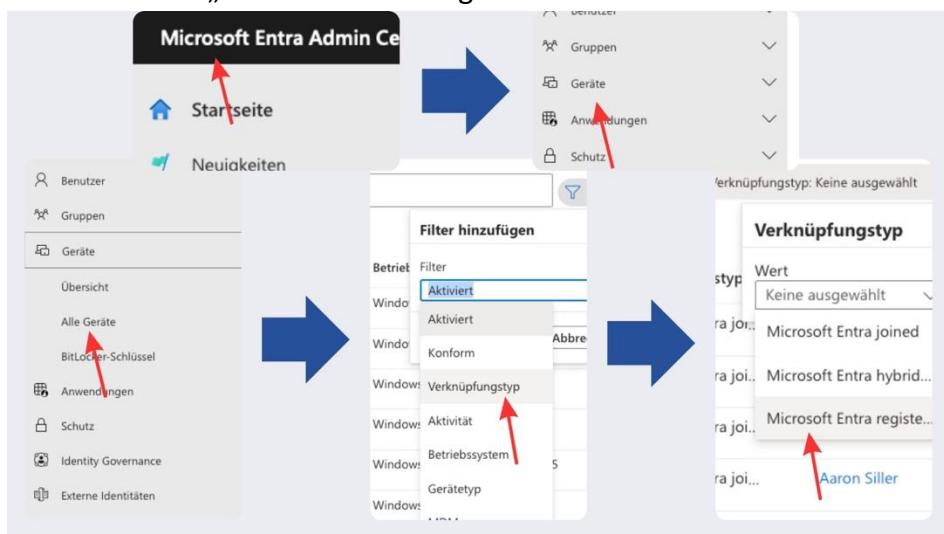


Bild 35: Validierung registrierter Geräte

Nun siehst du alle Geräte, die als „registered“ geführt werden – darunter fallen beispielsweise **iOS- und Android-Geräte**, die sich häufig im „Entra registered“-Zustand befinden. Das ist grundsätzlich in Ordnung.

Prüfe nun gezielt die **Windows-Geräte**. Achte auf ungewöhnliche Namen, private Geräte oder doppelte Einträge – z. B. von Terminalservern oder Geräten, die aufgrund wechselnder primärer

Benutzer mehrfach auftauchen. Dies kann Hinweise darauf geben, ob unerwünschte oder überzählige Geräte registriert wurden.

Solche Fälle sind in der Praxis keine Seltenheit. Insbesondere geteilte Systeme – wie Terminalserver oder Schulungsrechner – werden häufig mehrfach registriert, abhängig davon, welcher Benutzer sich jeweils anmeldet. Auch persönliche Geräte von Mitarbeitenden tauchen vereinzelt auf, wenn Benutzer sich etwa mit privaten Geräten am Unternehmens-Account anmelden. Diese solltest du regelmäßig prüfen und ggf. bereinigen.

Veraltete Geräte erkennen, deaktivieren und bereinigen

Im Microsoft Entra Admin Center gibt es die Möglichkeit, Geräte zu identifizieren, die seit längerer Zeit nicht mehr aktiv sind. Diese Funktion hilft bei der Bereinigung veralteter Einträge und trägt zur Übersichtlichkeit und Sicherheit der Umgebung bei.

Unter Microsoft Entra ID > Geräte > Alle Geräte findet sich eine Übersicht aller registrierten Geräte. Hier kann auch die Gesamtanzahl sowie der Status der einzelnen Geräte eingesehen werden. Besonders hilfreich ist die Kategorie „**Veraltete Geräte**“, welche Geräte auflistet, die sich, **seit mehr als sechs Monaten nicht mehr gegenüber Entra ID authentifiziert haben**.

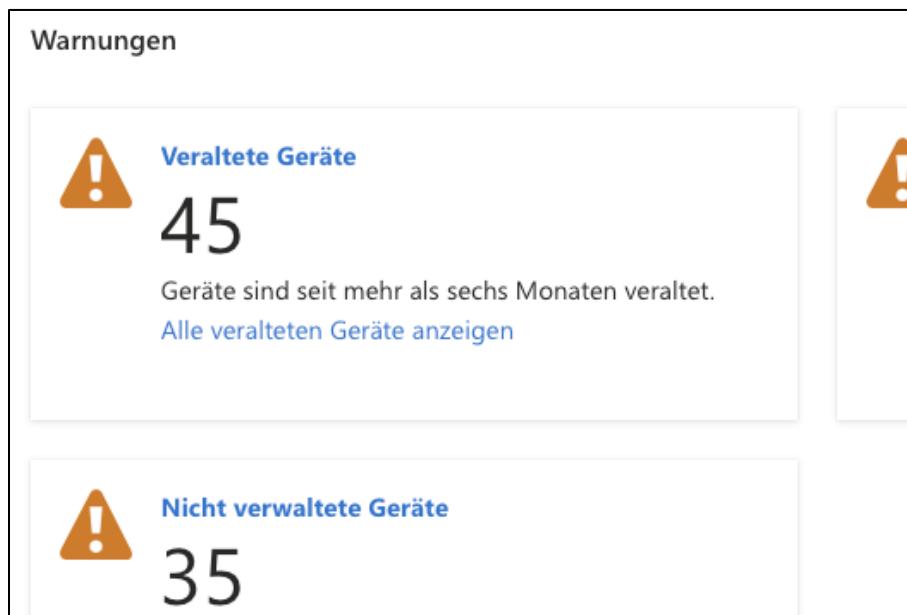


Bild 36: Veraltete Geräte

Hinweis:

Der Status „veraltet“ ist nicht immer ein verlässlicher Indikator dafür, dass das Gerät tatsächlich nicht mehr verwendet wird. In der Praxis kommt es vor, dass Geräte weiterhin aktiv sind, jedoch der Synchronisierungsdienst auf dem Gerät nicht mehr korrekt funktioniert – insbesondere, wenn das Gerät **nicht über Intune verwaltet** wird. Der betroffene Benutzer bemerkt dies oft nicht.

Empfohlene Vorgehensweise

1. Geräte nach Aktivität sortieren
- In der Liste der veralteten Geräte kann über die Spalte „Letzte Aktivität“ nach Datum sortiert werden – von alt nach neu.
2. Validierung vor Deaktivierung
- Gehe Eintrag für Eintrag durch und prüfe, ob das Gerät möglicherweise noch aktiv genutzt wird (z. B. durch Rückfrage beim Benutzer oder anhand von Metadaten).
- Ist klar, dass das Gerät nicht mehr benötigt wird, kann es deaktiviert werden.
3. Gerät deaktivieren
- Markiere das gewünschte Gerät
- Klicke auf „Deaktivieren“
- Bestätige die Aktion

Auswirkung auf den Benutzer:

Sobald ein deaktiviertes Gerät erneut gestartet wird, erscheint beim Benutzer alle 30 Minuten ein Hinweisfenster mit der Meldung:

„**Ihr Administrator hat dieses Gerät deaktiviert. Bitte wenden Sie sich an Ihre IT.**“

Die Nutzung des Geräts bleibt zwar grundsätzlich möglich, aber der Hinweis wird regelmäßig eingeblendet – was meist zur zeitnahen Rückmeldung durch den Benutzer führt.

4. Automatisierte Bereinigung (optional)

- Für größere Umgebungen empfiehlt sich die Automatisierung der Bereinigung über ein PowerShell-Skript in einem Azure Automation Runbook
- Dieses kann z. B. regelmäßig Geräte identifizieren, die seit über 180 Tagen inaktiv sind, und sie automatisch löschen

Wer die Kosten für Azure Automation vermeiden, kann auch manuell arbeiten:

5. Manuelle Bereinigung mit Wartezeit
- Geräte zunächst deaktivieren
 - Nach einer Wartezeit von z. B. vier Wochen prüfen, ob es Rückmeldungen gab
 - Anschließend endgültig löschen, wenn keine Nutzung mehr erfolgt

Kapitel 11: Benutzereinwilligungen und Schatten-IT kontrollieren

Navigiere im Microsoft Entra Admin Center auf der linken Seite zunächst in den Bereich „**Mehr anzeigen**“. Von dort wechselst du zu „**Anwendungen**“ und wählst dann „**Unternehmensanwendungen**“. In diesem Abschnitt findest du den wichtigen Unterpunkt „**Einwilligung und Berechtigung**“.

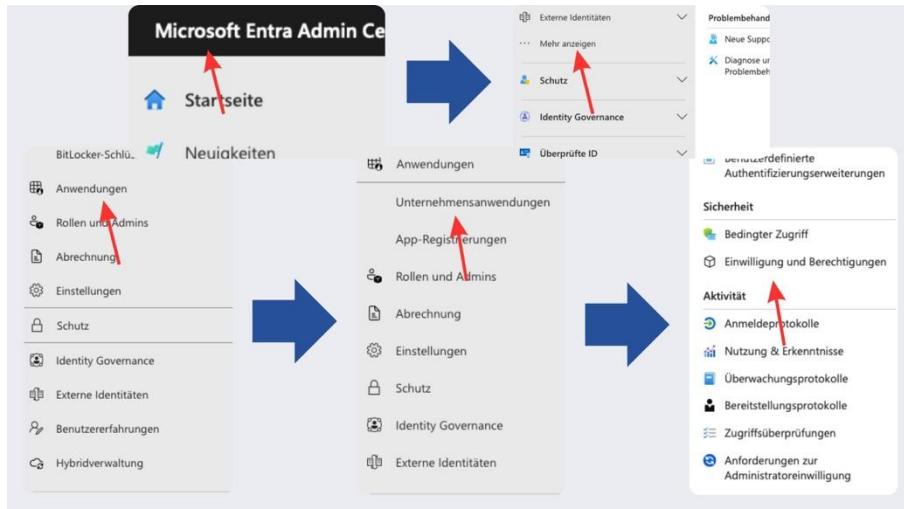


Bild 37: Unternehmensanwendungen

Hier steuerst du, ob Benutzer die Berechtigung haben, **Einwilligungen für Anwendungen selbst zu erteilen**. Dir stehen drei Konfigurationsoptionen zur Verfügung, die unterschiedliche Freiheitsgrade definieren:

1. Benutzereinwilligung nicht zugelassen
2. Für ausgewählte Berechtigungen die Benutzereinwilligung für Apps von verifizierten Herausgebern zulassen
3. Benutzereinwilligung für alle Apps zulassen

Prüfe, welche der Optionen aktuell bei dir eingestellt ist.

Benutzereinwilligung für Anwendungen
Hiermit wird konfiguriert, ob Benutzer Anwendungen die Einwilligung zum Zugriff auf Organisationsdaten benötigen.

Benutzereinwilligung nicht zulassen
Für alle Apps ist ein Administrator erforderlich.

Für ausgewählte Berechtigungen die Benutzereinwilligung für Apps von verifizierten Herausgebern zulassen
Für als schwach eingestufte Berechtigungen können alle Benutzer ihre Einwilligung für Apps von verschiedenen Herausgebern erteilen.

Benutzereinwilligung für Apps zulassen
Alle Benutzer können für jede App in den Zugriff auf die Daten der Organisation einwilligen.

Bild 38: Benutzereinwilligung

Warum du Option 1 verwenden solltest:

In der Praxis solltest du dich auf **Option 1 – „Benutzereinwilligung nicht zulassen“** festlegen. Diese Einstellung ist besonders sicher, denn sie verhindert, dass Benutzer eigenständig neue Anwendungen registrieren oder diesen Zugriff auf die Informationen deines Microsoft 365 Tenants gewähren.

Bei **Option 3** wäre es hingegen möglich, dass ein Benutzer – sei es bewusst oder unbewusst – eine externe Applikation oder einen SaaS-Dienst (z. B. über eine Webseite oder eine lokal installierte Software) mit seinem Microsoft 365-Konto verbindet. Falls die betreffende Anwendung dies unterstützt, wird sie **automatisch im Entra ID als Anwendung registriert**. Dabei können auch **Informationen aus dem Tenant ausgelesen werden**, etwa Kontaktdaten oder der Benutzername – je nachdem, welche Berechtigungen die Anwendung verlangt.

Dieses Verhalten möchtest du in der Regel **vermeiden**, denn es bedeutet Kontrollverlust über die eingesetzten Applikationen. Die Anmeldung geschieht oft über ein einfaches Popup-Fenster – für den Benutzer nicht als sicherheitsrelevanter Vorgang erkennbar.

Wenn du Einwilligungen auf Option 1 beschränkst und ein Benutzer versucht, eine neue Anwendung zu autorisieren, wird ihm folgendes angezeigt:

„Sie benötigen die Zustimmung eines globalen Administrators.“

In diesem Fall ist deine Zustimmung als Administrator erforderlich. Du musst dich einmalig mit deinem Global-Admin-Konto anmelden und die App aktiv freigeben. Dadurch stellst du sicher, dass **nur genehmigte Anwendungen** Zugriff auf deinen Tenant erhalten.

Analyse der vorhandenen Anwendungen

Nimm dir an dieser Stelle bitte ein paar Minuten Zeit und öffne die Übersicht unter „**Alle Anwendungen**“. Dort kannst du analysieren, welche Applikationen derzeit im Tenant registriert

sind. Schau dir genau an, ob darunter Anwendungen sind, die **du nicht erwartest**, hättest oder die **nicht durch dich freigegeben** wurden.

-  Eigenschaften
-  Besitzer
-  Rollen und Administratoren
-  Benutzer und Gruppen
-  Einmaliges Anmelden
-  Bereitstellung
-  Self-Service
-  Benutzerdefinierte Sicherheitsattribute

Gettin

Diese Analyse kann dir erste Hinweise auf „**Shadow IT light**“ liefern – also Dienste, die von Benutzern eingebunden wurden, ohne dass es eine zentrale Genehmigung gab. Auch wenn es sich nicht um klassische Schatten-IT im Sinne externer Systeme handelt, ist dies ein potenzielles Risiko für Compliance und Sicherheit.

Sicherheit

-  Bedinater Zuarifft

Bild 39: Benutzer und Gruppen

Links im Menü von der jeweiligen Anwendung findest du den Punkt „**Benutzer und Gruppen**“. Hier kannst du einsehen, welcher Benutzer eine Anwendung autorisiert hat. Diese Information ist hilfreich, wenn du Rückfragen stellen oder eine Anwendung gezielt entfernen möchtest.

Falls bei einer Anwendung kein Benutzer mehr hinterlegt ist, existiert das entsprechende Benutzerkonto unter Umständen nicht mehr. In solchen Fällen kannst du als Administrator die Anwendung dennoch analysieren und entsprechende Maßnahmen einleiten.

Für Anwendungen, die du **nicht weiter nutzen möchtest**, gehst du folgendermaßen vor:

1. Öffne die Eigenschaften der Anwendung
2. Setze die Anmeldung auf „**blockiert**“ – das heißt, es ist keine weitere Nutzung durch Benutzer mehr möglich
3. Warte ggf. einen definierten Zeitraum (z. B. 30 Tage), falls noch Rückfragen entstehen
4. Entferne die Anwendung anschließend aus dem Tenant

Dieses Vorgehen ist sauber und bietet dir gleichzeitig einen Puffer, um auf etwaige Reaktionen aus dem Benutzerkreis zu reagieren, bevor du Applikationen vollständig entfernst.

Kapitel 12: Plattformregistrierung in Intune einschränken

Wechsle zunächst in Intune und öffne das **Intune Admin Center**. Im linken Menü gehst du dann auf den Punkt „**Devices**“ und wählst anschließend „**Enrollment**“.

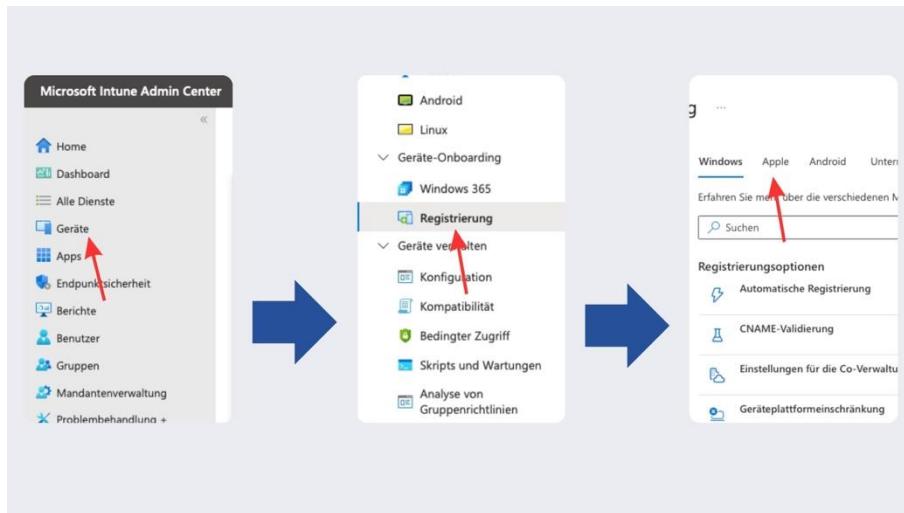


Bild 40: Enrollment

Hier beginnt die eigentliche Verwaltung der Geräteplattformen. Du bekommst nun eine Übersicht über die unterstützten Plattformen wie **Windows, Apple, Android** usw. Dies ist dein

zentraler Einstiegspunkt, um zu definieren, **wie und ob Geräte dieser Plattformen** bei dir im System registriert werden, dürfen.

Gehe jetzt in den Bereich „**Device Platform Restrictions**“ und wähle dort die Einstellung für „**All Users**“ aus. Im nächsten Schritt klickst du auf „**Properties**“ und findest dort die Option „**Platform Settings**“. Öffne diese mit „**Edit**“, um die Plattformrichtlinien zu bearbeiten.

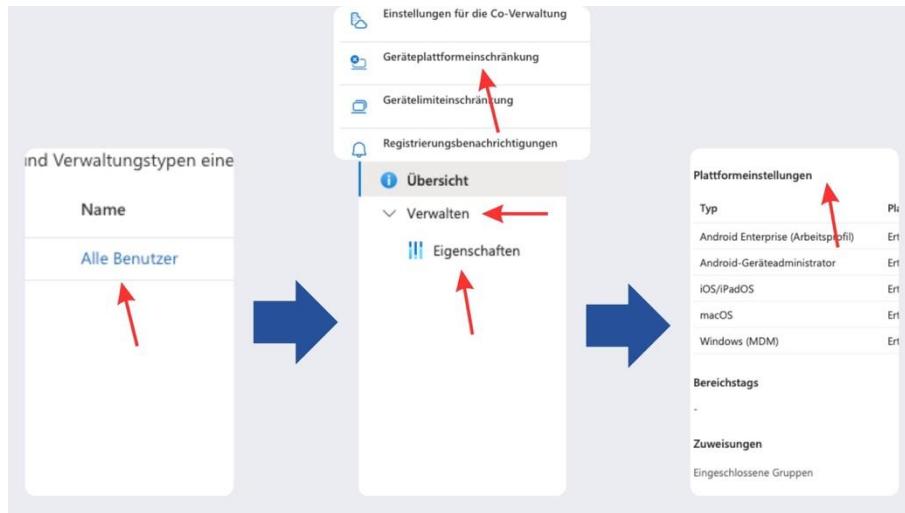


Bild 41: Device Platform Restrictions

Hier legst du konkret fest, **welche Gerätetypen in deinem Unternehmen für die Registrierung zugelassen** sind – und welche du **explizit blockierst**.

Ein besonders wichtiger Punkt: Wenn du Android-Geräte unterstützen möchtest, solltest du die Plattform „**Android Device Administrator**“ unbedingt **blockieren**. Dabei handelt es sich um die **veraltete MDM-Verwaltungsplattform von Google**, die schon lange **abgekündigt** wurde und **nicht mehr weiterentwickelt** wird.

Trotzdem wird sie in Microsoft Intune **immer noch unterstützt**. In manchen Fällen ist sie sogar noch die **voreingestellte** bzw. bevorzugte Option bei der Registrierung, je nachdem, welches Registrierungsprofil verwendet wird. Um zu vermeiden, dass Geräte über diese alte Methode eingebunden werden, solltest du diese Option konsequent auf „**Block**“ setzen.

Wenn du grundsätzlich keine Android-Geräte in deinem Unternehmen verwalten möchtest, kannst du Android **komplett deaktivieren**. Das gilt natürlich auch für alle anderen Plattformen. Beispiel: Wenn **macOS** für euch kein Thema ist, dann entferne macOS. Wenn ihr ausschließlich **iOS-Geräte** verwaltet, dann kannst du Windows und Android vollständig blockieren.

Das Ziel ist es, **nur die Plattformen zuzulassen, die du tatsächlich benötigst**, und alle anderen **konsequent auszuschließen**, um die Registrierung unerwünschter oder nicht verwalteter Geräte zu unterbinden.

In der Übersicht siehst du außerdem, dass es für jede Plattform eine Einstellung für „**Personally owned**“ gibt. Dabei handelt es sich um Geräte, die **nicht dem Unternehmen gehören**, sondern durch „**Bring Your Own Device**“-Szenarien (**BYOD**) von Mitarbeitenden eingebracht werden.

Wenn du eine Plattform blockierst – etwa **Android Device Administrator** oder **macOS** – dann wird automatisch auch der Zugriff von **personally owned devices** dieser Plattform unterbunden. Umgekehrt bedeutet das: Für Plattformen, die du aktiv erlaubst, bleibt der **Zugriff über private Geräte** zunächst möglich, sofern du dies nicht anderweitig über Richtlinien regulierst.

Ob ein Gerät als „**Personally Owned**“ (**BYOD**) registriert wird, hängt davon ab, **wie** du die Registrierung durchführst – also über welches Profil oder welche Anwendung. Das entscheidet über den Eigentumsstatus des Geräts im Intune-System.

Ein typisches Beispiel: Wenn du ein iOS-Gerät über das Unternehmensportal registrierst, erfolgt die Registrierung als **persönliches Gerät**. In solchen Fällen ist es also notwendig, **den Besitzstatus manuell auf „Unternehmen“ zu ändern**, falls gewünscht.

Bevor du das aber machst, solltest du dir gut überlegen, **ob der gewählte Registrierungsweg überhaupt zu deinem Use Case passt**. Eventuell gibt es einen anderen Weg, der besser geeignet ist – etwa für den Plattformtyp, das Sicherheitsmodell oder die Nutzergruppe. Das gilt nicht nur für iOS, sondern natürlich auch für **Android** und **Windows**.

Ein Hinweis an dieser Stelle: Wenn du mit Geräten arbeitest, die bereits im System sind, gilt diese Änderung **nur für neue Geräte**. Bestehende Geräte sind von den Änderungen **nicht betroffen**.

In Intune kannst du außerdem über die erweiterten Einstellungen **Mindest- und Maximalversionen des Betriebssystems festlegen** oder definieren, **welche Hersteller zugelassen** werden sollen. Auch das gehört zur Kontrolle darüber, **welche Gerätetypen du zulassen möchtest**. Es lohnt sich, hier klare Regeln zu setzen – je nach IT-Sicherheitsrichtlinie deines Unternehmens.

Navigiere erneut zu **Device Enrollment** im Intune Admin Center. Dort findest du die Einstellung „**Device Limit Restrictions**“. Öffne den Bereich „**All Users**“ → „**All Devices**“ → „**Properties**“ → „**Edit**“, um die Gerätekennzahlen anzupassen.

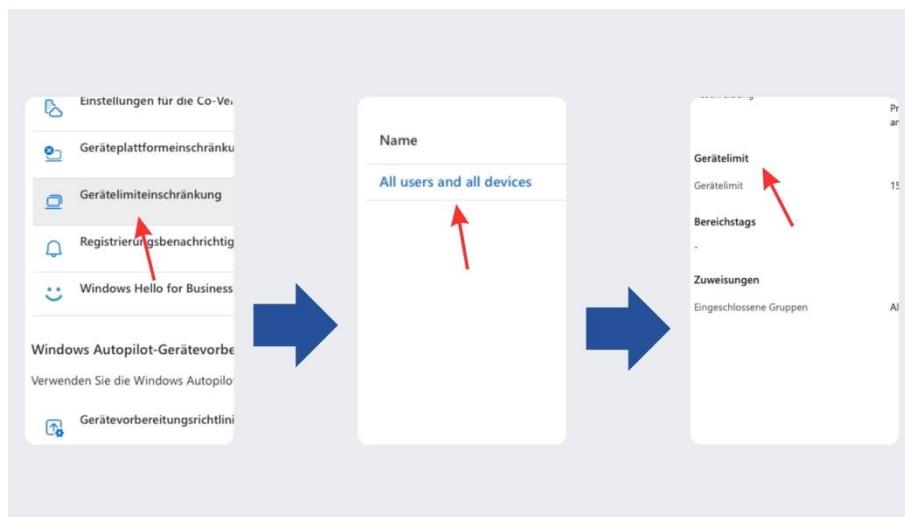


Bild 42: Gerätelimit

Standardmäßig liegt das **Device Limit pro Benutzer bei fünf Geräten**. Diese Grenze ist von Microsoft neu gesetzt worden. Überlege dir, ob du wirklich fünf Geräte pro Benutzer benötigst. In vielen Fällen reichen **ein bis zwei Geräte völlig aus**.

Wenn du das Limit reduzierst, gilt: **Bestandsgeräte bleiben registriert**, aber **neue Geräte können erst hinzugefügt werden, wenn ein altes entfernt oder entkoppelt wurde**.

Ein wichtiger technischer Punkt: Ob das Gerätelimit eines Benutzers überschritten wird oder nicht, hängt davon ab, **wer als „Primary User“** auf dem Gerät hinterlegt ist. Der **primäre Benutzer ist derjenige, der das Gerät registriert hat**.

Wenn du dir also im Intune Admin Center ein registriertes Gerät ansiehst, kannst du überprüfen, **welcher Benutzer als primär eingetragen** ist. Dieser Eintrag ist der **entscheidende Faktor**, ob das Gerät als eines der „limitierten“ Geräte für diesen Benutzer zählt. Du hast natürlich die Möglichkeit, diesen Eintrag manuell zu ändern.

Sollte es doch einmal nötig sein, dass ein Benutzer **mehr als das standardmäßige Limit** an Geräten registrieren darf, hast du die Möglichkeit, über „**Create Restrictions**“ individuelle Regeln zu definieren. Damit kannst du etwa einem bestimmten Benutzer erlauben, mehr Geräte zu registrieren als der Rest der Organisation. Diese Einstellung kann gezielt auf einzelne Benutzer angewendet werden.

Ein weiteres wichtiges Element ist der sogenannte „**Device Enrollment Manager**“. Du findest diese Option ebenfalls unter **Device Enrollment**, oben rechts im Menü.

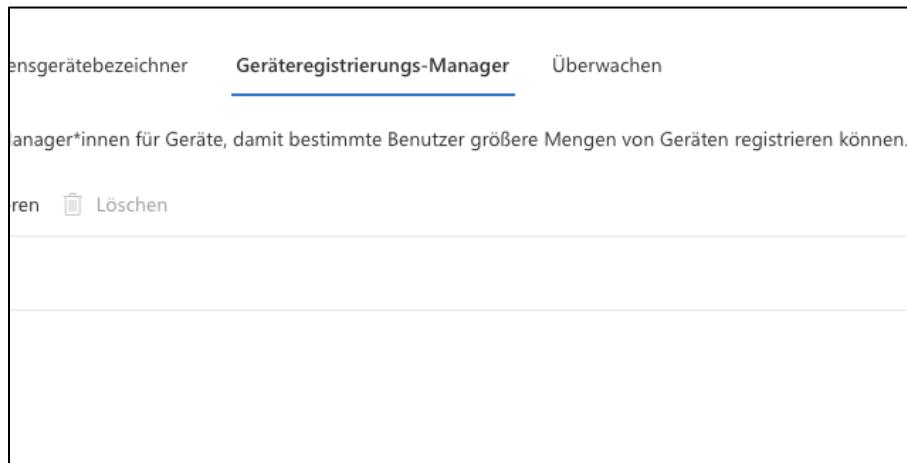


Bild 43: Geräteregistrierungs-Manager

Hier kannst du einen oder mehrere Benutzer hinterlegen, die als Device Enrollment Manager agieren dürfen. Diese Benutzer können dann **bis zu 1000 Geräte registrieren**. Dies ist besonders nützlich, wenn du z. B. einen IT-Mitarbeiter oder Dienstleister hast, der für viele Geräte verantwortlich ist.

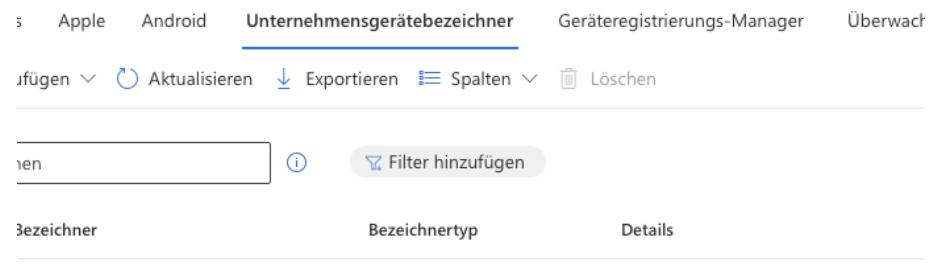
Beachte: Microsoft hat bewusst Einschränkungen eingebaut, um Missbrauch zu vermeiden. Zu den wichtigsten Limitierungen gehören:

Nur bestimmte Gerätetypen werden unterstützt: Ein DEM kann z. B. bis zu zehn unternehmenseigenen Geräten mit Arbeitsprofil oder vollständig verwaltete Geräte registrieren. Für BYOD-Szenarien (Bring Your Own Device) sind bis zu **1000 Registrierungen** möglich.

Nicht unterstützt werden:

- Apple Business Manager
- Android Open Source Project (AOSP)
- Lizenzverwaltung innerhalb Intune
- **Conditional Access** funktioniert nur ab einer bestimmten Version.
- **WiFi-Anmeldung** ist lediglich über **Zertifikate** möglich, nicht über Benutzeranmeldeinformationen (Credentials).
- **Keine Mehrfachnutzung:** Der DEM-Account ist nicht für die Verwendung durch mehrere Benutzer vorgesehen. Individuelle Zugriffskonzepte oder Personalisierungen sind in diesem Szenario nicht möglich.

Die zweite Funktion, die in diesem Zusammenhang von Bedeutung ist, nennt sich **Corporate Device Identifiers**. Diese findest du im Intune Admin Center unter dem gleichnamigen Menüpunkt. Mit dieser Funktion kannst du bestimmte Geräte **vorab autorisieren**, also auf eine **Whitelist setzen**, damit nur diese sich registrieren dürfen – insbesondere im Kontext von BYOD.



Filtern (i) Filter hinzufügen

Details

Bild 44: Unternehmensgerätebezeichner

Klicke hierzu auf **Add** und dann auf **Enter manually**. Im folgenden Schritt wählst du den **Identifier Type**, also die Art der Kennung, mit der das Gerät eindeutig identifiziert werden soll. Zur Auswahl stehen:

- E-Mail-Adresse
- Seriennummer

Sobald ein Gerät anhand einer dieser Kennungen registriert ist, wird es als **genehmigt** angesehen. Das bedeutet konkret: Du kannst auf Basis dieser Whitelist die generelle Registrierung von BYOD-Geräten **blockieren**, aber gleichzeitig gezielt Ausnahmen definieren – für Geräte, die du im Vorfeld anhand von Seriennummern oder E-Mail-Adressen freigibst.

Diese Methode bietet dir eine präzise Steuerungsmöglichkeit, um unautorisierte BYOD-Geräte aus deiner Umgebung auszuschließen, ohne komplett auf BYOD zu verzichten.

Wichtiger Hinweis: In der Praxis ist ein häufiges Problem, dass Unternehmen keine vollständige oder gepflegte Übersicht über Seriennummern oder E-Mail-Zuweisungen ihrer Geräte haben. Die Nutzung dieser Funktion setzt voraus, dass du genau weißt, welche Geräte du zulassen willst – und diese Information auch verlässlich dokumentiert ist.

Sollte das in deinem Fall gegeben sein, ist die Nutzung der Corporate Device Identifiers ein **effektives Werkzeug**, um eine sichere und kontrollierte Geräteverwaltung zu gewährleisten.

Funktion	Zweck	Einschränkungen / Hinweise
Device Enrollment Manager	Ermöglicht einem Benutzer, bis zu 1000 Geräte zu registrieren	Kein Apple Business Manager, keine Lizenzverwaltung, kein AOSP
Corporate Device Identifiers	Whitelisting von Geräten über E-Mail oder Seriennummer	Geräteliste muss vorliegen und gepflegt sein

Tablle 5: Übersicht der Funktionen

Kapitel 13: Windows Autopilot – Grundlagen und praktische Umsetzung

Der grundlegende Gedanke hinter Windows Autopilot ist es, den Prozess der Gerätbereitstellung so weit wie möglich zu automatisieren. Ziel ist es, dass ein Endanwender ein neues Gerät erhält, dieses auspakt, einschaltet, sich anmeldet und das Gerät anschließend automatisch alle relevanten Konfigurationen, Anwendungen und Richtlinien erhält – ohne dass ein IT-Administrator manuell eingreifen muss.

Damit dieses Vorgehen funktioniert, ist eine wichtige Voraussetzung, dass die sogenannte *Hardware ID* des Geräts vorab erfasst und registriert wurde. Die Hardware ID ist eine Kombination aus Seriennummer und einem Hashwert und kann vom Hardwarelieferanten ausgelesen werden. Idealerweise arbeitet dein Unternehmen mit einem oder wenigen zentralen Hardwarelieferanten zusammen, die diesen Prozess für euch übernehmen können. Der Lieferant kann die Hardware ID entweder direkt an euch übermitteln – z. B. per E-Mail – oder sie automatisiert in Intune hochladen. Die Hardware ID wird anschließend in Intune registriert, wo du die Verwaltung des Geräts vorbereiten kannst.

Wenn ein Gerät mit einer hinterlegten Hardware ID ausgeliefert wird, kann es direkt an den Endanwender verschickt werden. Der Nutzer öffnet das Paket, startet das Gerät, verbindet sich mit dem WiFi und meldet sich an. Im Hintergrund wird das Gerät automatisch in den sogenannten *Self-Deploying-Modus* versetzt. In diesem Modus erhält es alle für den Benutzer vorgesehenen Applikationen, Sicherheitsrichtlinien und Konfigurationen.

Es ist wichtig zu verstehen, dass Intune im Rahmen von Autopilot keine vollständige Neuinstallation des Betriebssystems durchführt. Stattdessen wird das vorhandene Windows-

Image genutzt und angepasst. Das bedeutet, dass das bestehende System-Image bestehen bleibt, während Intune alle Konfigurationen über das Internet – genauer gesagt über das Content Delivery Network (CDN) von Microsoft – auf das Gerät ausrollt.

Der Erfolg dieses automatisierten Bereitstellungsprozesses hängt stark davon ab, wie gut die zugewiesenen Anwendungen und Richtlinien im Vorfeld definiert sind. Du solltest dabei differenzieren, welche Anwendungen zwingend erforderlich sind und daher sofort installiert werden müssen, und welche Anwendungen optional sind und vom Benutzer später bei Bedarf installiert werden können.

Microsoft Endpoint Manager – Automatisches Deployment mit AutoPilot

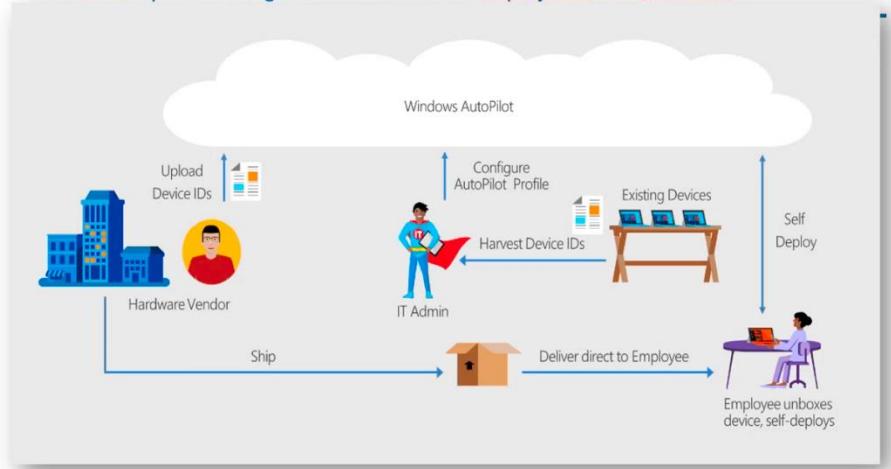


Bild 45: Microsoft Endpoint Manager

Da die Konfiguration ausschließlich über das Internet erfolgt, kann der Downloadumfang erheblich sein – in manchen Fällen bis zu 80 oder 100 Gigabyte. Wenn dann keine ausreichende Bandbreite zur Verfügung steht, kann sich das Deployment über mehrere Stunden hinziehen. Es ist also essenziell, einen praktikablen Mittelweg zu finden zwischen sofortiger Einsatzfähigkeit und Hintergrundinstallation von weniger kritischen Komponenten.

Eine weitere Möglichkeit besteht darin, dass das Gerät zunächst zu dir in die IT-Abteilung geliefert wird. Dort kannst du beim Startvorgang durch fünfmaliges Drücken der Windows-Taste den sogenannten *Free-Cash-Modus* aktivieren. In diesem Modus werden alle benötigten Applikationen und Richtlinien bereits heruntergeladen und vorkonfiguriert. Anschließend kannst

du das Gerät dem Benutzer übergeben. Der muss dann lediglich noch die Kontoeinrichtung vornehmen. Dieser Vorgang kann das Deployment auf wenige Minuten reduzieren. Alternativ kann auch der Hardwarelieferant diesen Schritt übernehmen, wenn du den gesamten Prozess auslagern möchtest.

Die Registrierung der Hardware ID ist zwingend erforderlich. Ohne diese Hardware ID funktioniert Autopilot im Hybrid-Join-Szenario nicht. Auch beim reinen Cloud-Join treten ohne korrekt hinterlegte Hardware ID regelmäßig Probleme auf. Wenn dir jemand sagt, dass Autopilot auch ohne Hardware ID funktioniert, solltest du dem nicht folgen – in der Praxis ist ein erfolgreicher Ablauf ohne diese Voraussetzung nicht zuverlässig möglich.

Microsoft bewirbt Autopilot mit dem Versprechen eines ortsunabhängigen Deployments – *Deployment from anywhere*. Das ist grundsätzlich korrekt, bringt aber bei der Nutzung des *Hybrid-Join* einige technische Anforderungen mit sich. Sobald sich der Benutzer am Gerät anmeldet und auf den Windows-Desktop zugreift, ist eine aktive Verbindung zum lokalen Active Directory notwendig. Dafür benötigst du eine VPN-Lösung, die eine geräte- oder zertifikatsbasierte Authentifizierung unterstützt. Eine reine Benutzername-Passwort-Authentifizierung reicht hier nicht aus.

Zwar gäbe es Workarounds über die Eingabeaufforderung mit *Shift+F7* und manuelle Kommandos, jedoch sind diese nicht für Endanwender geeignet. Für den Einsatz von Autopilot im Hybrid-Join ist daher eine geeignete VPN-Lösung unumgänglich. Microsoft bietet hierfür eine eigene Lösung an, aber auch andere Anbieter liefern entsprechende Produkte. Letztlich bedeutet dies, dass das Deployment in Hybrid-Szenarien häufig weiterhin innerhalb des Unternehmensnetzwerks erfolgt. Das kann für dich völlig in Ordnung sein, sollte aber bei der Planung berücksichtigt werden.

Für Bestandsgeräte besteht ebenfalls die Möglichkeit, Autopilot zu nutzen.

Manuelles Auslesen per Script:

Du kannst ein PowerShell-Script verwenden, um die Hardware ID eines Geräts manuell auszulesen. Dieses Script kann lokal ausgeführt oder beispielsweise via Gruppenrichtlinie (GPO)

auf mehreren Geräten gleichzeitig eingesetzt werden. Die erzeugten Hardware IDs kannst du dann beispielsweise zentral auf einem Netzlaufwerk ablegen.

Sobald ein Gerät zurückgesetzt wurde, kannst du es auf dieser Basis erneut über Autopilot bereitstellen.

Automatisches Auslesen über Intune:

Alternativ bietet Microsoft mittlerweile auch die Möglichkeit, dass Intune die Hardware IDs dynamisch ausliest. Voraussetzung dafür ist, dass die betreffenden Geräte bereits im Entra ID registriert und entsprechenden Gruppen zugewiesen sind. Diese Funktion erleichtert die Bereitstellung insbesondere bei Bestandsgeräten erheblich und macht eine manuelle Sammlung der Hardware IDs überflüssig.

Ein weiterer technischer Aspekt betrifft die Dauer des Deployments im Hybrid Join. Da hier zwei voneinander getrennte Computerkonten erstellt werden – eines im lokalen Active Directory und eines in Entra ID – müssen diese am Ende miteinander verknüpft werden. Diese Synchronisierung erfolgt in einem späten Schritt des Prozesses und kann erheblich Zeit in Anspruch nehmen. In Extremfällen hat dieser Vorgang bis zu 48 Stunden gedauert.

Durch das Überspringen der grafischen Darstellung des Fortschritts lässt sich die Dauer signifikant verkürzen – teilweise auf etwa zwei Stunden. Dennoch bleibt eine sorgfältige Vorabplanung entscheidend: Welche Applikationen sind kritisch? Welche Datenmengen werden übertragen? Wie stark ist die Bandbreite vor Ort?

In einigen Umgebungen ist bereits eine andere Lösung für die Softwareverteilung im Einsatz – beispielsweise Barramundi. Im direkten Vergleich zeigt sich häufig, dass klassische Softwareverteilungslösungen wie Barramundi bei der Anwendungsbereitstellung performanter und zuverlässiger arbeiten als Intune. Das bedeutet jedoch nicht, dass das Autopilot-Konzept grundsätzlich ungeeignet ist – vielmehr hängt die Qualität der Umsetzung maßgeblich von der Planung, Bandbreite und Systemintegration ab.

Kapitel 14: Zentrale Enrollment-Einstellungen und Windows Hello for Business in Intune

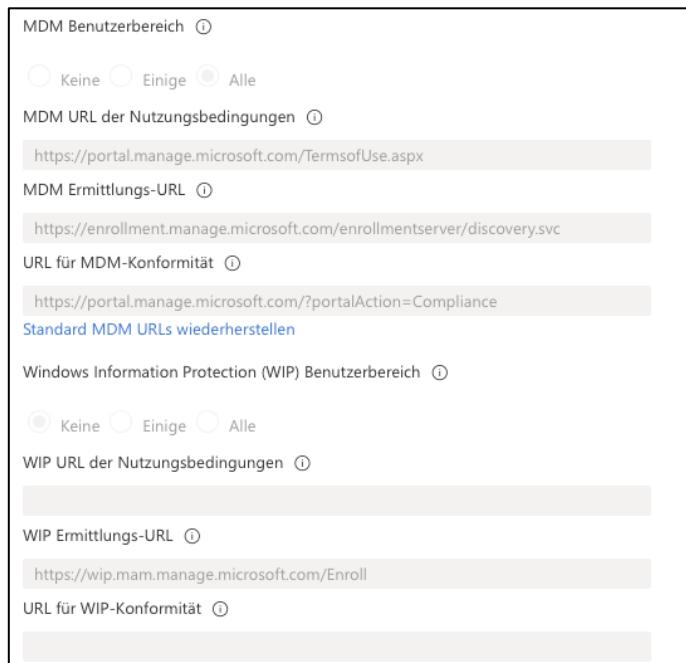
Im Microsoft Intune Admin Center lassen sich zentrale Einstellungen für die automatische Geräteverwaltung vornehmen, insbesondere im Hinblick auf die Registrierung von Windows-Geräten über Autopilot. Dafür navigiert man zunächst in den Bereich **Devices** und anschließend zu **Enrollment > Automatic Enrollment**.



Bild 46: Automatische Registrierung

Zwei zentrale Konfigurationspunkte sind hier der **MDM User Scope** und der **Windows Information Protection (WIP) Scope**. Der MDM Scope bestimmt, welche Benutzer berechtigt sind, Geräte automatisch über Intune registrieren zu lassen. Es stehen die Optionen **Some** – zur Beschränkung auf bestimmte Azure AD-Gruppen – oder **All** für die vollständige Freigabe zur Verfügung. Welche Einstellung gewählt wird, hängt davon ab, welche Benutzer im Unternehmen Geräte über Autopilot registrieren dürfen.

Der darunterliegende Windows Information Protection Scope kann in den meisten Fällen auf



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 ⓘ

None belassen werden, da die Aktivierung auch zu einem späteren Zeitpunkt an anderer Stelle erfolgen kann. Grundsätzlich gilt: Ein Gerät, das in MDM registriert ist, ist auch automatisch für den Einsatz von WIP vorbereitet.

Bild 47: MDM & WIP

Ein weiterer relevanter Konfigurationspunkt ist die sogenannte **CName Validation**, die sich ebenfalls im Enrollment-Bereich befindet.

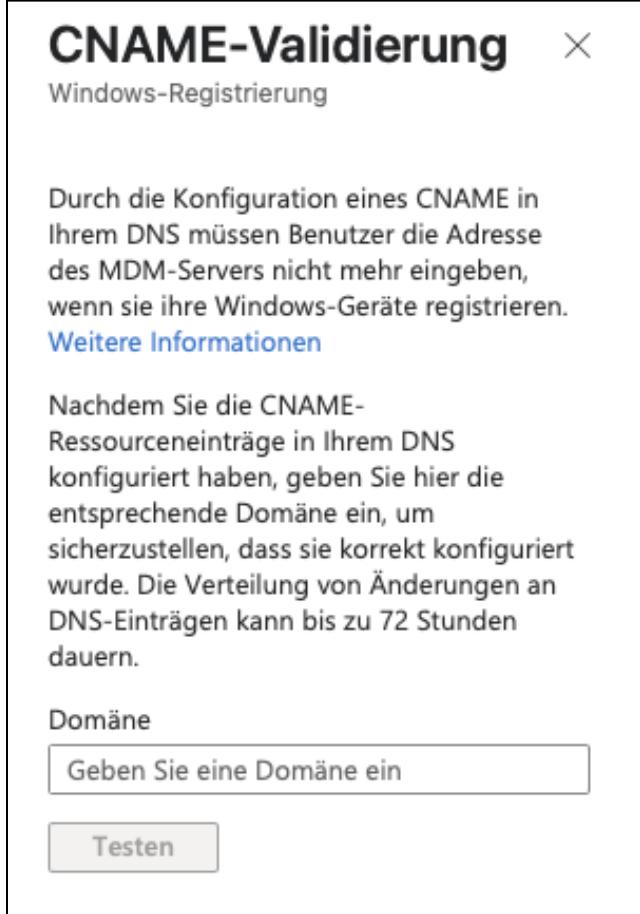


Registrierungsoptionen	
	Automatische Registrierung Hiermit konfigurieren Sie die Registrierung
	CNAME-Validierung Hiermit wird die CNAME-Registrierung
	Einstellungen für die Co-Verwaltung Co-Verwaltungseinstellungen für die C
	Geräteplattform einschränkung Konfigurieren, welche Plattformversion
	Gerätemaxlimiteinschränkung Definieren Sie, wie viele Geräte jeder Be
	Registrierungsbenachrichtigungen E-Mail- oder Pushbenachrichtigungen

Bild 48: CNAME-Validierung

Hier wird eine Domain hinterlegt, meist basierend auf dem verwendeten UPN-Suffix. Dies dient der Verifikation, dass die über Intune ausgerollten Geräte mit einer gültigen Domäne verknüpft sind. Es empfiehlt sich, diesen Wert testweise zu prüfen, um sicherzustellen, dass die im Tenant verwendete Domäne mit der bei der Gerätebereitstellung aktiven Domäne übereinstimmt. Sollte der Wert nicht korrekt erkannt werden, ist eine manuelle Prüfung der Domänen-

konfiguration notwendig, insbesondere im Hinblick auf DNS-Einträge und eventuelle fehlende Simion-Einträge.



The screenshot shows a window titled "CNAME-Validierung" with a close button. Below the title is the subtitle "Windows-Registrierung". The main text explains that through CNAME configuration in the DNS, users can register their Windows devices without entering the MDM server address. It includes a link to "Weitere Informationen". The text continues to describe the process of entering the domain name after configuring CNAME entries in the DNS. A "Domäne" label is followed by an input field containing "Geben Sie eine Domäne ein" and a "Testen" button.

Bild 49: Domäne

Der Bereich **Co-Management** kann übersprungen werden, sofern im Unternehmen kein Microsoft Configuration Manager im Einsatz ist. Wesentlich interessanter sind dagegen die **Enrollment Notifications**, die optional eingerichtet werden können. Sie bieten eine komfortable Möglichkeit, Benutzer nach Abschluss der Gerätebereitstellung zu informieren – etwa durch eine Toast-Benachrichtigung oder eine E-Mail. Die Funktion befindet sich ebenfalls im Enrollment-Bereich und kann über **Create Notification** eingerichtet werden.



Bild 50: Registrierungsberechtigung

Ein weiterer Punkt in der Windows-Geräteverwaltung über Intune ist die Integration von **Windows Hello for Business (WHfB)**. Intune prüft automatisch, ob die jeweilige Hardware WHfB unterstützt, und versucht bei Vorhandensein geeigneter Komponenten diese Funktion zu aktivieren. Im Admin Center lässt sich WHfB unter **Windows Enrollment > Windows Hello for Business** konfigurieren. Die Standardeinstellung ist oft auf „Not configured“ gesetzt, wodurch das System die Benutzer bei der Anmeldung fragt, ob sie Hello for Business nutzen möchten. Administratoren können diese Entscheidung jedoch auch zentral vorgeben – entweder durch Deaktivierung (**Disabled**) oder durch explizite Aktivierung (**Enabled**).

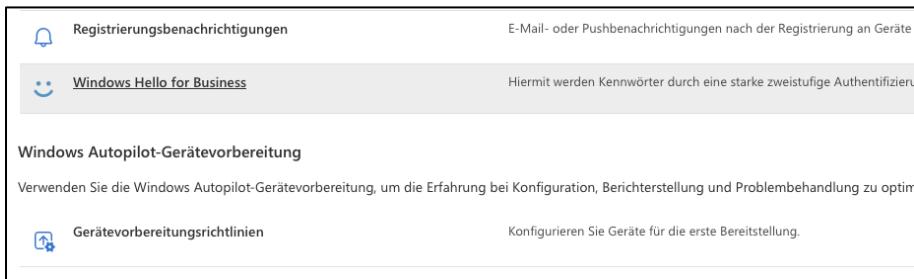


Bild 51: WHfB

Wird WHfB aktiviert, greift im Fehlerfall ein sogenanntes Fallback-Szenario: Die Anmeldung erfolgt dann per PIN. Diese PIN kann durch spezifische Richtlinien abgesichert werden, etwa durch Anforderungen an Länge, Groß- und Kleinschreibung, Sonderzeichen und Gültigkeitsdauer. Obwohl eine PIN nicht denselben Sicherheitsstandard wie WHfB selbst bietet, stellt sie dennoch ein notwendiges und funktionales Backup dar. Es besteht auch die Möglichkeit, die PIN-Nutzung vollständig zu deaktivieren und ausschließlich WHfB zuzulassen. Dies erhöht jedoch das Risiko, im Fehlerfall keine Anmeldung durchführen zu können, sollte WHfB einmal nicht funktionieren.

Windows Hello for Business konfigurieren: ⓘ	Aktiviert
Trusted Platform Module (TPM) verwenden: ⓘ	Erforderlich Bevorzugt
PIN-Mindestlänge: ⓘ	6
Maximale PIN-Länge: ⓘ	127
Kleinbuchstaben in PIN: ⓘ	Nicht zulässig
Großbuchstaben in PIN: ⓘ	Nicht zulässig

Bild 52: PIN

WHfB gilt allgemein als eine der sichersten im Microsoft-Umfeld verfügbaren Zwei-Faktor-Authentifizierungsmethoden, auch wenn sie nicht vollständig phishingresistent ist. Sie erreicht jedoch ein Schutzniveau, das sehr nah an die wirklich phishingresistenten Faktoren herankommt. Deutlich unsicherer – aber dennoch weit verbreitet – sind Authentifizierungsmethoden wie SMS oder Telefonanruf. Laut Microsoft konnten aber selbst diese Methoden im Rahmen einer Sicherheitskonferenz im Sommer des Vorjahres etwa 94 Prozent aller Angriffe erfolgreich abwehren. Auch wenn die Einführung von Zwei-Faktor-Authentifizierung im Unternehmensumfeld organisatorisch herausfordernd sein kann, bleibt ihr Mehrwert im Sicherheitskontext unbestritten.

Ein wichtiger Hinweis zur Konfiguration von WHfB ist, dass sich die Einstellungen an mehreren Stellen innerhalb des Intune Admin Centers finden lassen. Neben dem globalen Bereich unter **Windows Enrollment** kann WHfB auch in **Konfigurationsprofilen** oder im Bereich **Endpoint Security** gesteuert werden. Diese parallelen Konfigurationsmöglichkeiten sind historisch gewachsen. Es empfiehlt sich daher, eine einheitliche Strategie zur Verwaltung und Durchsetzung dieser Sicherheitstechnologie zu entwickeln.

Kapitel 15: Windows Autopilot Deployment Profiles

Du arbeitest dabei im Microsoft Intune Portal und nutzt die Möglichkeiten von AutoPilot, um Windows-Geräte effizient bereitzustellen. Aktuell solltest du allerdings von der Funktion „Windows Autopilot Device Preparation“ noch Abstand nehmen. Auch wenn diese Funktion bei ihrer Ankündigung als mögliche Nachfolgeversion von Autopilot interpretiert wurde, ist sie in der Praxis bislang ausschließlich auf Cloud-only-Geräte ausgerichtet. Sie bietet derzeit keine vollwertige Alternative zu den etablierten Deployment Profiles, insbesondere wenn hybride Szenarien berücksichtigt werden müssen. Für den Moment empfiehlt es sich daher, bei den klassischen Autopilot Deployment Profiles zu bleiben.

Beginne den Konfigurationsprozess, indem du in Intune den Bereich „Devices“ aufrufst und dort unter „**Device-Onboarding**“, „**Registrierung**“, „**Windows**“ den Punkt „**Deployment Profiles**“ auswählst.



Bild 53: Bereitstellungsprofile

Dort hast du die Möglichkeit, über „Create Profile“ ein neues Profil anzulegen. Für die folgenden Schritte konzentrierst du dich auf die Geräteplattform „Windows PC“. Die Plattform „HoloLens“ ist in diesem Zusammenhang nicht relevant.

Im ersten Schritt gibst du dem Profil einen eindeutigen Namen. Dieser kann beispielsweise ein Kürzel enthalten, um später besser zuordnen zu können, welchem Gerätetyp oder Szenario das Profil zugewiesen ist. Zusätzlich kannst du eine Beschreibung hinzufügen. Die Einstellung „Convert all targeted devices to Autopilot“ – also die Umwandlung aller Zielgeräte in AutoPilot-

Geräte – solltest du auf „Yes“ setzen. Der Hintergrund: Wenn du das Profil später einer Azure AD Gruppe zuweist, die Geräte enthält, die noch keine registrierte Hardware-ID besitzen, wird über diese Einstellung automatisch die Hardware-ID gesammelt und registriert. Dies ist ein wichtiger Bestandteil des AutoPilot-Workflows, da es dir erlaubt, Geräte ohne manuelles Hochladen der Hardware-ID bereitzustellen.

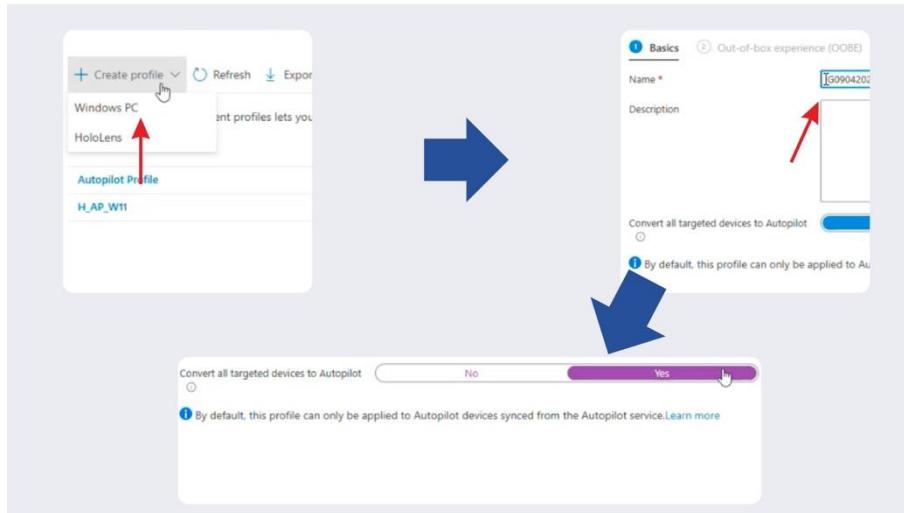


Bild 54: AutoPilot Profil

Nach dem Benennen und Beschreiben des Profils gehst du im Assistenten auf „Next“, um mit der Konfiguration fortzufahren. Im nächsten Schritt definierst du den Bereitstellungsmodus („Deployment mode“). Hier gibt es zwei Optionen: „User driven“ und „Self-deploying“. Du solltest dich zunächst auf „User driven“ konzentrieren. Diese Variante ist für Geräte gedacht, die einzelnen Benutzern zugewiesen sind. Die „Self-deploying“-Option ist hingegen für Geräte im KIOSK-Modus vorgesehen.

Anschließend legst du fest, wie das Gerät der Microsoft Entra ID beitreten soll. Hier hast du zwei Optionen: „Microsoft Entra joined“ oder „Microsoft Entra hybrid joined“. Je nachdem, welche Variante du auswählst, ändern sich die Konfigurationsoptionen leicht. Wenn du „Microsoft Entra hybrid joined“ auswählst, erscheint zusätzlich der Punkt „Skip AD connectivity check“. Dieser lässt sich auf „Yes“ oder „No“ setzen. In hybriden Umgebungen kann es sinnvoll sein, diese Prüfung zu überspringen, insbesondere wenn du weißt, dass die Verbindung zur lokalen Active Directory Domäne gewährleistet ist. Bei Auswahl der hybriden Join-Variante ist zudem das Feld „Apply device name template“ ausgegraut.

Deployment mode * ⓘ	User-Driven
Join to Microsoft Entra ID as * ⓘ	Microsoft Entra hybrid joined
Skip AD connectivity check ⓘ	No Yes
Microsoft Software License Terms ⓘ	Show Hide
ⓘ Important information about hiding license terms	
Privacy settings ⓘ	Show Hide
ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.	
Hide change account options ⓘ	Show Hide
User account type ⓘ	Administrator Standard
Allow pre-provisioned deployment ⓘ	No Yes
Language (Region) ⓘ	Operating system default
Automatically configure keyboard ⓘ	No Yes
Apply device name template ⓘ	No Yes
For Microsoft Entra hybrid joined type of Autopilot deployment profiles, devices are named using ⌂ settings specified in Domain Join configuration.	

Bild 55: Entra Hybrid Joined

Der grundsätzliche Gedanke hinter dieser Konfiguration ist es, den Rollout-Prozess für die Endanwender so einfach wie möglich zu gestalten. Je weniger Eingaben erforderlich sind, desto geringer ist die Fehleranfälligkeit beim *Deployment*. Daher sollte das *Deployment*-Profil so gestaltet werden, dass es möglichst viele Einstellungen automatisch übernimmt und den Benutzer eine reduzierte Zahl an Entscheidungen abverlangt.

Create profile ...

Windows PC

Basics **Out-of-box experience (OOBE)** Assignments Review + create

Configure the out-of-box experience for your Autopilot devices

Deployment mode *	User-Driven
Join to Microsoft Entra ID as *	Microsoft Entra joined
Microsoft Software License Terms	Show  Hide
<small>Important information about hiding license terms</small>	
Privacy settings	Show  Hide
<small>The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.</small>	
Hide change account options	Show  Hide
User account type	Administrator  Standard
Allow pre-provisioned deployment	No  Yes
Language (Region)	Operating system default
Automatically configure keyboard	No  Yes
Apply device name template	No  Yes
Create a unique name for your devices. Names must be 15 characters or less, and can contain letters (a-z, A-Z), numbers (0-9), and hyphens. Names must not contain only numbers. Names cannot include a blank space. Use the %SERIAL% macro to add a hardware-specific serial number. Alternatively, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.	
Enter a name *	%SERIAL%

Bild 56: Deployment-Profil

Nach diesen Schritten findest du eine weitere Option mit der Bezeichnung „Allow pre-provisioned deployment“. Wenn du diese Option aktivierst, kann ein IT-Administrator oder ein Dienstleister das Gerät vollständig vorbereiten, bevor es an den Endnutzer ausgeliefert wird. Das spart Zeit und ermöglicht einen reibungslosen Übergang, da der Benutzer direkt mit einem fertigen System arbeiten kann. Die Aktivierung dieser Funktion ist in jedem Fall empfehlenswert – selbst wenn sie nicht aktiv genutzt wird. Sie verursacht keine Probleme, und ihre spätere Nutzung ist ohne erneute Profiländerung möglich. Aktiv bleibt die Funktion ohne Wirkung, solange sie nicht explizit verwendet wird.

Allow pre-provisioned deployment	No  Yes
Language (Region)	Operating system default
Automatically configure keyboard	No  Yes
Apply device name template	No  Yes
Create a unique name for your devices. Names must be 15 characters or less, and can contain letters (a-z, A-Z), numbers (0-9), and hyphens. Names must not contain only numbers. Names cannot include a blank space. Use the %SERIAL% macro to add a hardware-specific serial number. Alternatively, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.	

Bild 57: Allow pre-provisioned deployment

Im Anschluss daran folgen weitere Konfigurationspunkte. Die Einstellung „**Language (user select)**“ legt fest, ob der Benutzer während der Bereitstellung die Betriebssystemssprache selbst wählen kann. Dies ist besonders dann nützlich, wenn ein Unternehmen Geräte in mehreren Sprachen ausliefert – etwa in international tätigen Firmen. Wird diese Option aktiviert, kann der Nutzer zwischen den verfügbaren Sprachen wählen. Standardmäßig sind oft Englisch und die jeweilige Landessprache vorinstalliert; alle weiteren Sprachen werden bei Bedarf nachinstalliert. Dies verlängert jedoch die Installationszeit geringfügig. Wenn kein Bedarf besteht, kann die automatische Auswahl auch deaktiviert werden.

Auch die **Tastaturlayout-Einstellung („Automatic Keyboard“)** sollte aktiviert werden, um automatisch das passende Layout bereitzustellen. Dies trägt zur Vereinfachung des Setups bei und reduziert Benutzereingriffe auf ein Minimum.

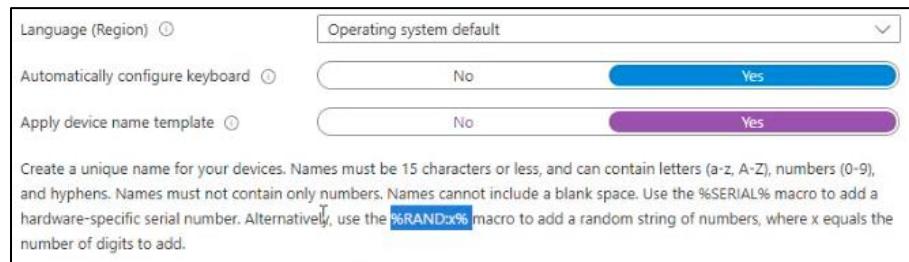


Bild 58: Language und Keyboard

Ein weiterer Punkt ist die Einstellung „**Apply device name template**“, mit der ein Namensschema für bereitgestellte Geräte definiert werden kann. Bei einem Kundenprojekt wurde beispielsweise festgelegt, dass die Geräte automatisch mit einem Namen versehen werden, der sich aus der Seriennummer bis zum 15. Zeichen zusammensetzt. Diese Methode ist funktional, jedoch stößt die Namensvergabe in Intune schnell an ihre Grenzen.

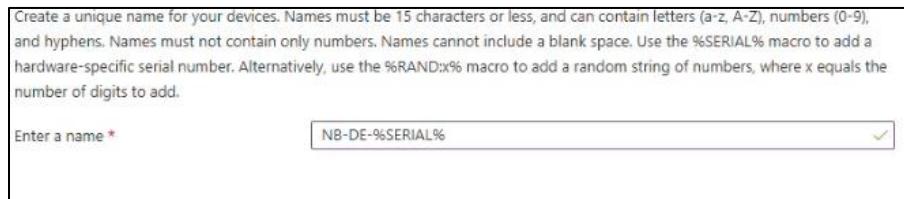
Die Vorgaben von Microsoft sind hier relativ eingeschränkt:

- Der Geräte-Name darf maximal 15 Zeichen lang sein.
- Er darf Buchstaben, Zahlen und bestimmte Sonderzeichen enthalten.
- Es gibt zwei verfügbare Variablenarten:
- **%SERIAL%**: Die Seriennummer des Geräts.
- **%RAND:x%**: Eine zufällig generierte Zahl mit x Stellen (z. B. **%RAND:3%** ergibt dreistellige Zufallszahlen wie 103, 297, 481 usw.)

Dabei ist besonders zu beachten, dass die Zufallszahl nicht sequentiell erzeugt wird. Wer also anhand der Endziffern den Gerätezeitpunkt oder das Alter eines Geräts ableiten möchte, wird hier keine verlässliche Reihenfolge erzielen können.

Die Verwendung der Seriennummer ist grundsätzlich sinnvoll, insbesondere für Unternehmen, die Geräte inventarisieren oder in einem zentralen Asset-Management führen. In anderen Szenarien hingegen – etwa wenn die Seriennummer optisch schwer erfassbar ist oder schlicht keine Rolle spielt – kann diese Namensgebung als hinderlich empfunden werden.

Unternehmen mit komplexeren Anforderungen an die Gerätebenennung – etwa nach Schema „NB-DE-123“ für ein Notebook aus Deutschland mit eindeutiger Nummer – stoßen hier an die Grenzen eines einzelnen Autopilot-Profil. Denn: Für jede Namenskonvention müsste ein eigenes Profil angelegt werden. Alternativ ist es möglich, die Gerätenamen nachträglich manuell oder automatisiert über ein Skript zu ändern. Ob sich dieser Mehraufwand lohnt, hängt vom jeweiligen Unternehmenskontext ab. Für kleine Unternehmen mit wenigen Geräten pro Monat (z. B. 5 Geräte) ist eine manuelle Umbenennung meist vertretbar. In größeren Umgebungen oder bei einem hohen Automatisierungsgrad hingegen empfiehlt sich der Einsatz von Skripten oder die Verwendung eines konsistenten Namensschemas innerhalb mehrerer spezifischen Deployment-Profile.



Create a unique name for your devices. Names must be 15 characters or less, and can contain letters (a-z, A-Z), numbers (0-9), and hyphens. Names must not contain only numbers. Names cannot include a blank space. Use the %SERIAL% macro to add a hardware-specific serial number. Alternatively, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.

Enter a name *

NB-DE-%SERIAL%

Bild 59: Device name template

Nutzung von dynamischen Gruppen

Ein weiterer Bestandteil der automatisierten Verwaltung in Microsoft Intune ist die Nutzung dynamischer Gruppen. Diese ermöglichen es, Geräte oder Benutzer auf Basis definierter Kriterien automatisch Gruppen zuzuweisen – etwa anhand von Geräteeigenschaften oder Benutzerattributen. Dadurch entfällt eine manuelle Zuordnung und es lassen sich Richtlinien sowie Konfigurationen gezielt und effizient anwenden.

In Intune Admin Center kannst du eine bestehende dynamische Gruppe überprüfen. Dazu navigierst du im Menü zu **Groups**, suchst nach dem Gruppennamen und wählst anschließend die entsprechende Gruppe aus. In der Detailansicht der Gruppe findet sich auf der linken Seite der Abschnitt **Dynamic Membership Rules**, in dem die aktuell geltende Regel eingesehen werden kann.

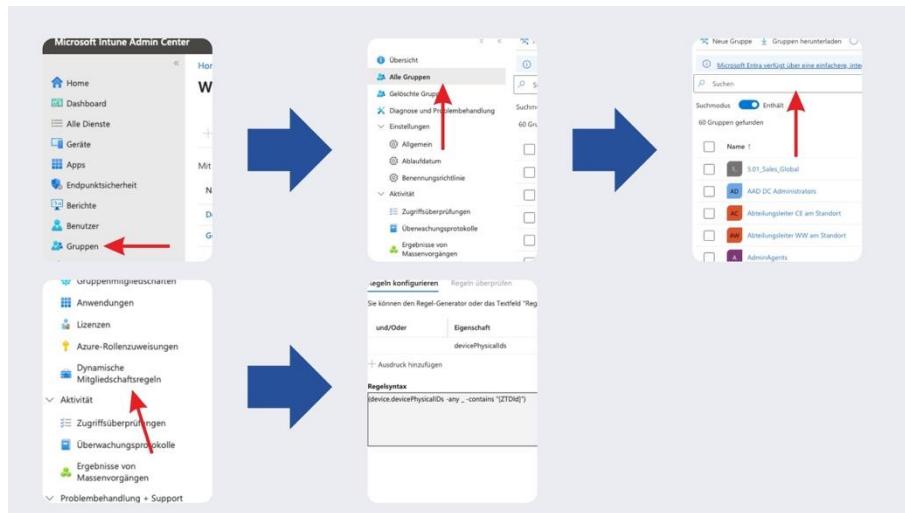


Bild 60: Dynamische Gruppenregeln

Für die gezielte Anwendung von Windows AutoPilot-Profilen ist die Verwendung dynamischer Gerätegruppen in Microsoft Intune erforderlich. Zwei zentrale Attribute spielen hierbei eine besondere Rolle: die sogenannte **Device Physical ID (ZTD-ID)** sowie die **Order ID**. Obwohl Microsoft in der Bezeichnung dieser Kennungen uneinheitlich vorgeht – die Begriffe Hardware ID, Device ID oder ZTD-ID meinen inhaltlich dasselbe –, ist der technische Hintergrund identisch: Es handelt sich um eine eindeutige Gerätekennung, die für die Verwaltung in AutoPilot-Prozessen essenziell ist.

Zunächst ist zu beachten, dass AutoPilot-Profile ausschließlich auf **Gerätegruppen**, nicht auf **Benutzergruppen**, angewendet werden sollten. Auch wenn das Intune-Interface theoretisch die Auswahl von Personengruppen zulässt, erfordert die ordnungsgemäße Bereitstellung über AutoPilot immer eine Gerätetruppenzuweisung. Über eine **Filterung**, welche auf dem Attribut `devicePhysicalIds -contains "[ZTD-ID]"` basiert, lassen sich automatisch alle Geräte erfassen, deren Hardware ID im Tenant hinterlegt wurde. Diese Regel filtert gezielt jene Geräte heraus,

die über eine gültige ZTD-ID verfügen und somit für ein Deployment über AutoPilot infrage kommen.

Darüber hinaus existiert die sogenannte **Order ID**, die auch unter dem Begriff **Group Tag** bekannt ist. Dieses Attribut ermöglicht eine differenzierte Kategorisierung von Geräten – zum Beispiel nach Standort, Abteilung oder Einsatzzweck. Die Order ID ist flexibel definierbar: Sie wird beim Hochladen der Hardware ID mitgegeben und dient später als Filterkriterium für die Gruppenzuweisung. Eine typische Regel könnte etwa wie folgt aussehen: (device.devicePhysicalIDs-any_-contains "[ZTDID]"). Dabei steht IT für eine frei wählbare Bezeichnung, die als Tag fungiert.



Bild 61: devicePhysicalIDs

Die Order ID ist insbesondere dann hilfreich, wenn im Unternehmen mehrere AutoPilot-Profile mit unterschiedlichen Konfigurationen benötigt werden – etwa zur Abbildung variierender Namenskonventionen, Netzwerkeinstellungen oder Applikationspakete. In diesem Fall wird pro gewünschtem Szenario eine separate Gerätgruppe mit entsprechend gefilterter Order ID angelegt, der dann das jeweils passende AutoPilot-Profil zugewiesen wird.

Zusammengefasst bedeutet das:

- ZTD-ID dient zur Identifikation aller Geräte mit hinterlegter Hardware ID.
- Order ID erlaubt die zielgerichtete Zuordnung von Geräten zu spezifischen Autopilot-Profilen basierend auf benutzerdefinierten Kriterien.

Diese Kombination aus dynamischer Gruppenzuweisung und gezieltem Profil-Mapping ist ein zentrales Element für den erfolgreichen Einsatz von AutoPilot in modernen Gerätebereitstellungsprozessen.

Konfiguration der Enrollment Status Page für AutoPilot-Deployments

Nach der Zuweisung eines Autopilot-Deployment-Profil auf eine dynamische Gerätegruppe, ist es erforderlich, zusätzlich die sogenannte **Enrollment Status Page (ESP)** zu konfigurieren. Diese Seite ist ein zentraler Bestandteil der Benutzererfahrung während der Ersteinrichtung eines Geräts über Autopilot und sollte in keinem Deployment-Profil fehlen.

Zur Konfiguration navigierst du im Intune Admin Center zu **Devices > Enrollment > Enrollment Status Page**. Dort wählst du die Einstellung **All Users and All Devices**, klickst auf **Properties** und anschließend auf **Settings**. In diesem Bereich legst du fest, wie sich die Statusanzeige während des AutoPilot-Prozesses verhalten soll.

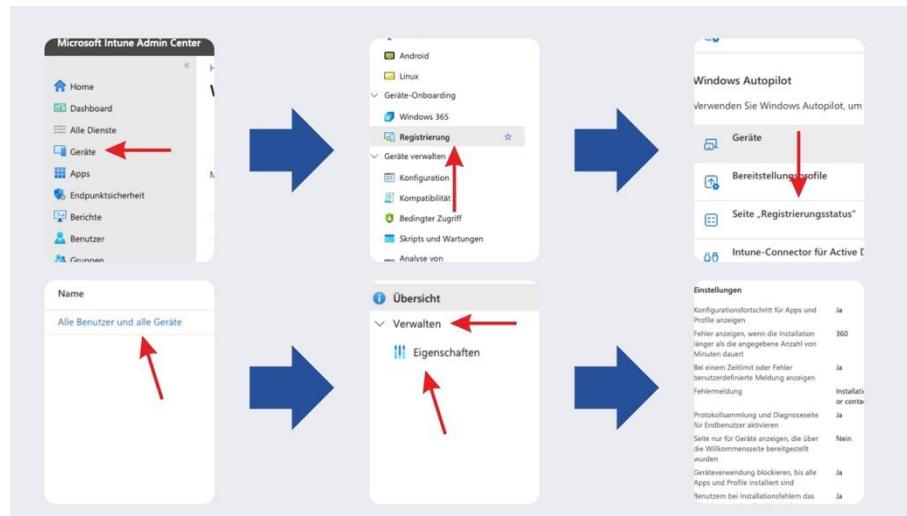


Bild 62: Enrollment Status Page

In der Praxis hat sich gezeigt, dass viele Organisationen, die ESP grundsätzlich aktiviert haben. Dabei bleibt die Konfiguration häufig weitgehend bei den Standardeinstellungen. Lediglich die unterste Einstellung „**Show an error when installation takes longer than specified number of minutes**“ ist auf „Selected“ gesetzt – mit einem Wert von **60 Minuten** als maximale Installationsdauer.

Diese Einstellung legt fest, nach welcher Zeitspanne ein Fehler angezeigt wird, wenn die Bereitstellung nicht abgeschlossen ist. Während 60 Minuten in manchen Umgebungen ausreichend sein mögen, empfiehlt sich in vielen Fällen ein **höherer Puffer**, beispielsweise **180 Minuten**. Damit wird vermieden, dass ein Deployment fälschlich als fehlerhaft abgebrochen wird, obwohl es lediglich durch langsame Netzwerkverbindungen oder größere Applikationspakete verzögert ist.



Bild 63: Zeitspanne Installation

Die Option „**Show Custom Message when Time Limit and Error**“ lässt sich verwenden, um eine benutzerdefinierte Nachricht anzuzeigen, sobald die maximale Zeit überschritten oder ein Fehler aufgetreten ist. Es empfiehlt sich, diese Nachricht an dein internes Wording anzupassen, sodass sie für die Anwender verständlich und im Ton deiner Organisation gehalten ist.

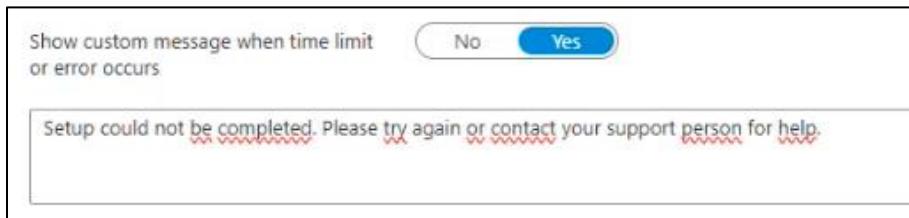


Bild 64: Show message

Die Einstellung „**Turn on log collection in diagnostic page for end users**“ solltest du auf „Yes“ setzen. Damit wird im Fehlerfall automatisch ein Dialogfenster geöffnet, das den Benutzer darauf hinweist, dass er die Logs einsehen kann. Das ist sowohl im Self-Deployment-Szenario als auch bei einer internen Gerätbereitstellung hilfreich, um Fehler schneller zu erkennen.

Turn on log collection and diagnostics page for end users

No

Yes

Bild 65: Log collection

Die Option „**Only show page to devices provisioned by out of box experience (OOBE)**“ solltest du auf „**Yes**“ setzen. Selbst wenn du den Großteil deiner Geräte über AutoPilot ausrollt, bietet es Flexibilität, die ESP auch dann anzuzeigen, wenn ein Gerät manuell oder außerhalb von OOBE bereitgestellt wird. So bleibt die Anzeige der Installationsfortschritte aktiv – unabhängig davon, auf welchem Weg das Gerät registriert wurde.

Die Enrollment Status Page selbst zeigt dem Benutzer während der Einrichtung an, wie viele Applikationen und Richtlinien bereits installiert bzw. angewendet wurden, z. B. „App 5/10“, „Richtlinie 7/11“. Wenn du dies nicht einstellst, wird diese Ansicht geskippt.

Only show page to devices provisioned by out-of-box experience (OOBE)

No

Yes

Bild 66: OOBE Page

Die Einstellung „**Block device use until all apps and profiles are installed**“ solltest du ebenfalls auf „**Yes**“ setzen. Damit wird sichergestellt, dass das Gerät nicht vorzeitig genutzt werden kann, bevor alle erforderlichen Anwendungen und Konfigurationsprofile vollständig bereitgestellt wurden.

Block device use until all apps and profiles are installed ⓘ

No

Yes

Bild 67: Block device

Auch „**Allow user to reset device if installation error occurs**“ sollte auf „**Yes**“ gesetzt werden. Diese Option zeigt dem Benutzer im Fehlerfall einen Button an, mit dem das Deployment zurückgesetzt und erneut gestartet werden kann. Das ist nicht nur für den Endanwender

hilfreich, sondern auch für dich im IT-Support, wenn z. B. ein Gerät vor Ort zurückgesetzt werden muss. Du sparst dir damit aufwendigere manuelle Schritte wie ein erneutes Imaging oder das manuelle Neustarten des Setups.

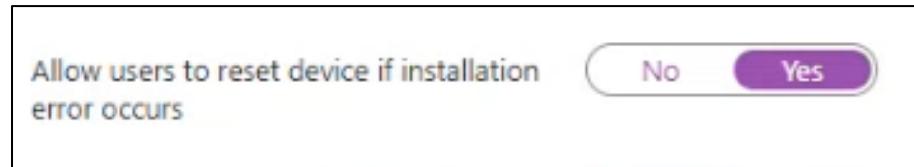


Bild 68: Reset error occurs

Die Option „**Allow user to use device if installation fails**“ hingegen solltest du konsequent auf „**No**“ setzen. Damit stellst du sicher, dass das Gerät bei einem fehlgeschlagenen Deployment nicht unkontrolliert in Betrieb genommen wird.



Bild 69: Use error occurs

Es sollte im jeweiligen Unternehmenskontext geprüft werden, welche Regelung für besser empfunden wird. Generell gilt: Die Konfiguration der Enrollment Status Page sollte immer auf die **technische Infrastruktur, Bandbreite, Komplexität der Richtlinien sowie Menge und Größe der Anwendungen** abgestimmt sein, um einen reibungslosen und benutzerfreundlichen Onboarding-Prozess sicherzustellen.

Einsatz der Enrollment Status Page zur Steuerung der Applikationsbereitstellung

Im Rahmen der Konfiguration deiner **Enrollment Status Page (ESP)** solltest du auch den Bereich „**Block device use until required apps are installed**“ gezielt anpassen.

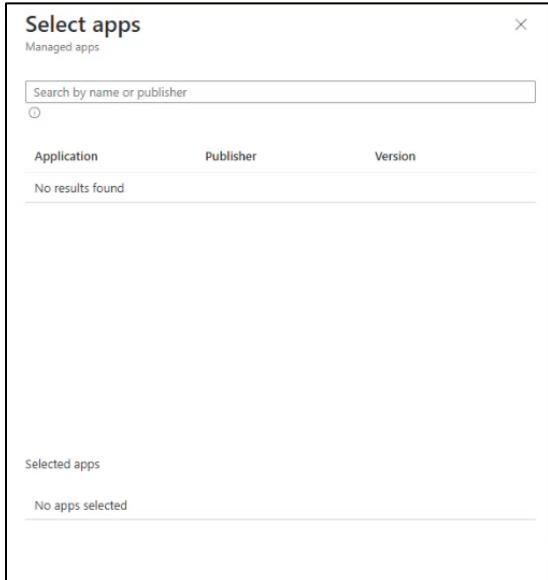
Block device use until required apps are installed if they are assigned to the user/device

All **Selected**

Bild 70: Required Apps

Hier empfiehlt es sich, die Einstellung auf „**Selected**“ zu setzen. Anschließend kannst du unter „**Select apps**“ genau festlegen, welche Applikationen auf dem Gerät zwingend installiert sein müssen, bevor der Benutzer das Gerät verwenden darf.

Bild 71: Select Apps



In deinem Tenant sind möglicherweise noch keine Applikationen hinterlegt. In dem Fall solltest du vorab definieren, welche Anwendungen für euch als „**Must-Have**“ gelten – also welche Applikationen unbedingt installiert sein müssen, damit ein Benutzer arbeitsfähig ist. Halte diese Auswahl so schlank wie möglich, um das Deployment nicht unnötig zu verzögern. Ein gängiger Ansatz, der sich in vielen Umgebungen etabliert hat, ist es, nur diese Kernanwendungen verpflichtend über die ESP auszurollen. Alle weiteren Programme können dann im Nachgang durch den Benutzer über das **Unternehmensportal** installiert werden.

Dazu kannst du die Unternehmensportal-App nutzen. Dort erscheint eine Übersicht verfügbarer Anwendungen, die der Benutzer per Klick installieren kann. Visuell lässt sich das ansprechender gestalten, z. B. mit Logos, aber auch eine einfache Listenansicht ist funktional ausreichend. Dieser zweistufige Bereitstellungsansatz – zunächst die wichtigsten Tools über die ESP, anschließend die weiteren über das Portal – ermöglicht einen kontrollierten Rollout bei gleichzeitig flexibler Nachinstallation.

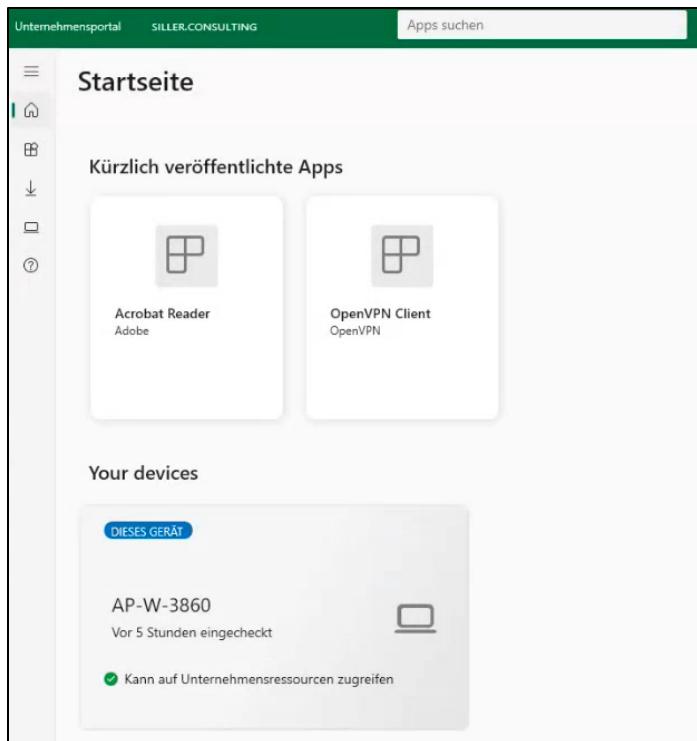


Bild 72: Unternehmensportal

Alternativ besteht auch die Möglichkeit, mehrere essentielle Applikationen über die ESP zu definieren, aber nur eine Teilmenge davon als „Blocking Criteria“ festzulegen. Das heißt, beispielsweise

fünf Anwendungen sind insgesamt vorgesehen, doch nur drei davon müssen zwingend vor der Nutzung installiert sein. Sobald diese drei erfolgreich bereitgestellt sind, erhält der Benutzer Zugriff auf den Desktop. Die verbleibenden Anwendungen werden im Hintergrund installiert.

Zur besseren Nachverfolgbarkeit solltest du in jedem Fall die **Enrollment Status Page** aktiviert lassen. Diese zeigt dem Benutzer – oder dir als IT-Administrator – transparent an, in welchem Abschnitt sich das Gerät gerade befindet: „**Device Preparation**“, „**Device Setup**“ und „**Account Setup**“. Diese Phasen werden grafisch dargestellt, typischerweise mit einem hellen Bildschirm unter Windows 11. Damit erkennst du jederzeit, wie weit der Installationsprozess fortgeschritten ist.

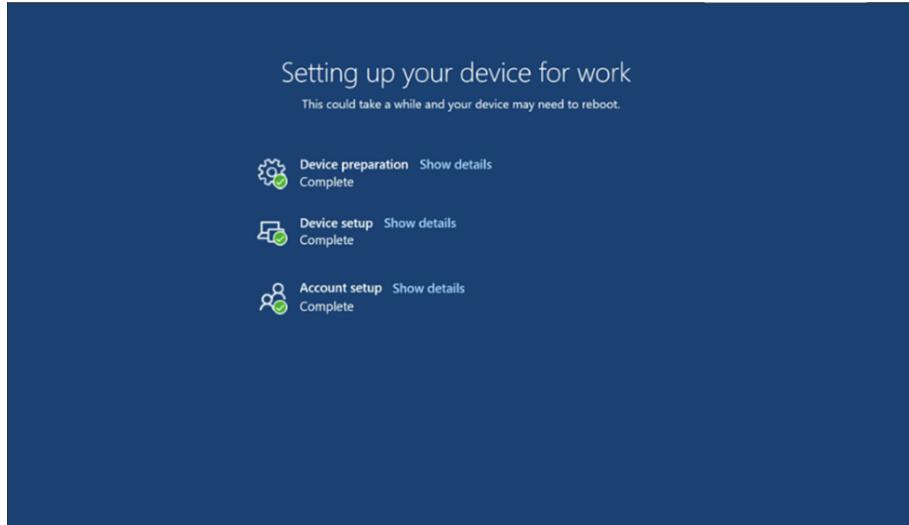


Bild 73: Setting up

Verzichtest du hingegen auf die ESP, wird der Benutzer direkt zum Windows-Desktop weitergeleitet. In der Praxis führt dies häufig zu Rückfragen seitens der Benutzer, etwa weil Anwendungen fehlen oder Richtlinien noch nicht angewendet wurden. Um solche Fälle zu vermeiden und die Installation vollständig nachvollziehbar zu gestalten, solltest du die Enrollment Status Page unbedingt aktivieren.

Manuelles Hochladen von Geräten in Windows Autopilot per PowerShell-Skript

Im Microsoft Intune Admin Center lassen sich Geräte für den Windows AutoPilot manuell vorbereiten, indem man die entsprechenden Hardwareinformationen über ein PowerShell-Skript erfasst und anschließend im Admin Center importiert. Dieser Prozess dient insbesondere dazu, **Bestandsgeräte nachträglich in AutoPilot einzubinden**, wenn sie nicht direkt durch einen Hardwarelieferanten registriert wurden.

In der praktischen Umsetzung wird hierfür zunächst das PowerShell-Skript zur Erfassung der AutoPilot-Daten verwendet. Dieses Skript erzeugt eine **CSV-Datei**, die folgende Informationen enthält:

- Device Serial Number: Die Seriennummer des physischen Geräts

- Windows Product ID: In der Regel leer
 - Hardware Hash: Ein 256-stelliger kryptografischer Hashwert, der zur eindeutigen Identifizierung des Geräts dient

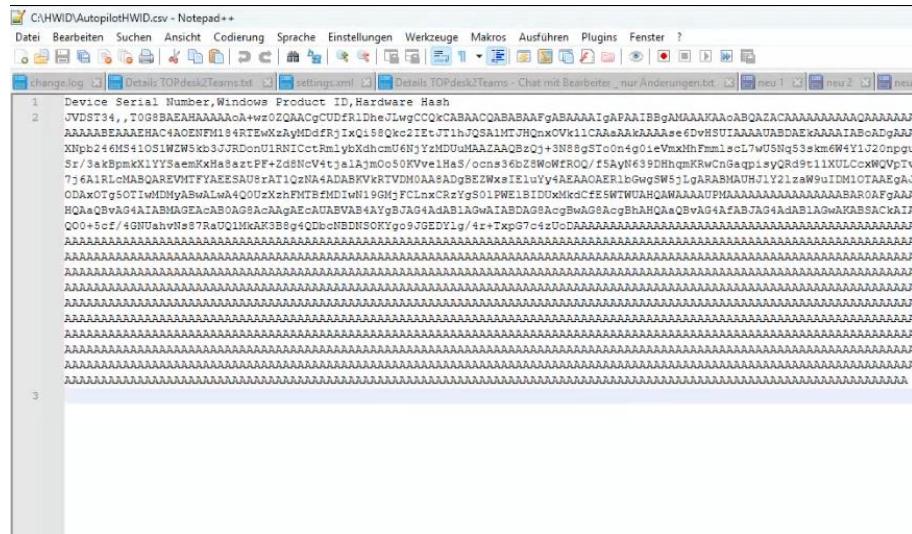


Bild 74: CSV Datei

Nach dem Ausführen des Skripts liegt die CSV-Datei lokal vor. Für die Zuweisung von Geräten zu bestimmten AutoPilot-Profilen kann zusätzlich eine **Order ID (auch Group Tag genannt)** verwendet werden. Diese wird manuell in der letzten Spalte der CSV-Datei ergänzt. Beispiel: Hinter die letzte Zeile in der Datei wird ,DE geschrieben, um dem Gerät etwa das Group Tag *DE* zuzuweisen.

Sobald die Datei vorbereitet ist, erfolgt der Upload im Intune Admin Center:

1. Navigiere zu Devices > Registrierung > Geräte
 2. Wähle Import aus und lade die vorbereitete CSV-Datei hoch
 3. Nach erfolgreichem Formatcheck (z. B. „ordnungsgemäß formatierte Zeilen: 1“) bestätigst du mit Importieren
 4. Intune zeigt an: Geräte werden importiert – der Prozess kann bis zu 15 Minuten dauern, ist aber meist schneller abgeschlossen

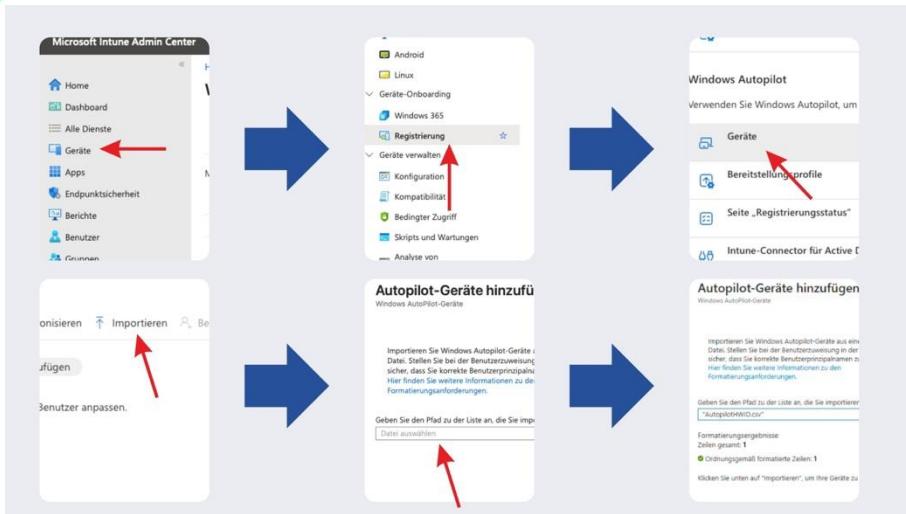


Bild 75: CSV-Datei importieren

Zuweisung von Autopilot-Profilen über Gruppentags und dynamische Gerätegruppen

Im Rahmen der Windows AutoPilot-Konfiguration in Microsoft Intune ist die korrekte Zuweisung von Geräten zu dynamischen Gruppen entscheidend, um Deployment-Profile automatisiert anwenden zu können. In diesem Zusammenhang spielt insbesondere der sogenannte **Gruppentag (Order ID)** eine zentrale Rolle.

Wenn du eine dynamische Gruppe für den Einsatz mit AutoPilot einrichten möchtest, kannst du dies direkt in Intune durchführen. Falls du noch keine entsprechende Gruppe angelegt hast, empfiehlt es sich, dies nachzuholen, um die Zuweisung von AutoPilot-Profilen zu automatisieren und gezielt Geräte zu verwalten.

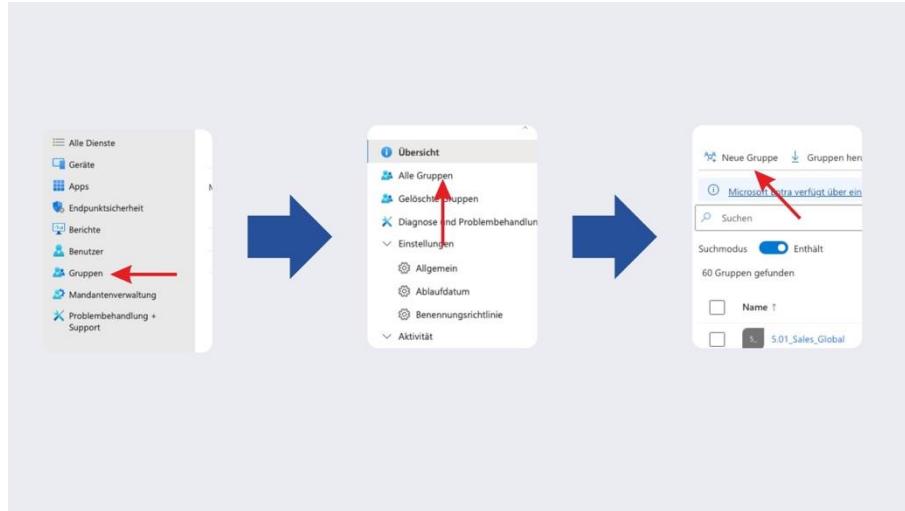
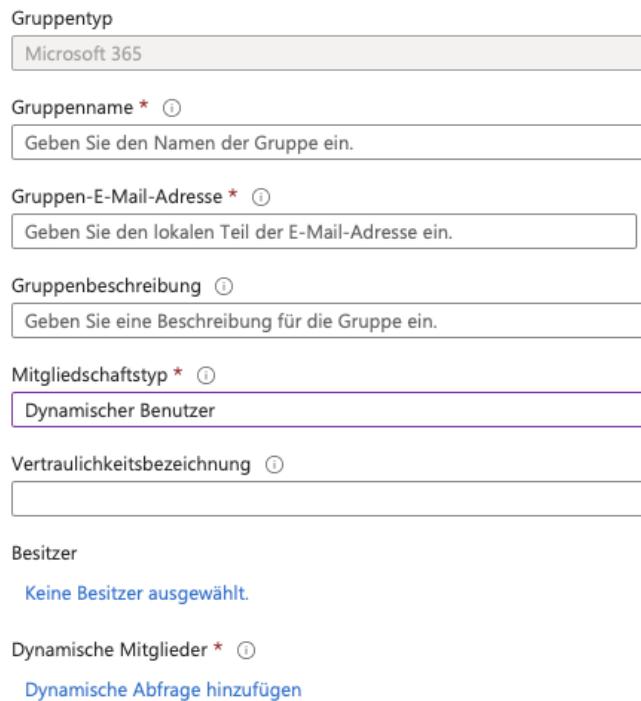


Bild 76: Dynamische Gruppe anlegen

Öffne dazu ein neues Browser-Tab und navigiere im Microsoft Intune Admin Center auf der linken Seite zu „**Alle Gruppen**“. Dort legst du eine neue Gruppe an. Wähle beim **Gruppentyp** eine „**Sicherheitsgruppe**“ und beim **Mitgliedschaftstyp** „**Dynamisches Gerät**“ aus. Diese Auswahl ist wichtig, damit sich Geräte automatisch anhand definierter Regeln zuordnen lassen.



The screenshot displays the "Gruppe definieren" (Define Group) form with the following fields:

- Gruppentyp:** Microsoft 365
- Gruppenname ***: Geben Sie den Namen der Gruppe ein.
- Gruppen-E-Mail-Adresse ***: Geben Sie den lokalen Teil der E-Mail-Adresse ein.
- Gruppenbeschreibung**: Geben Sie eine Beschreibung für die Gruppe ein.
- Mitgliedschaftstyp ***: Dynamischer Benutzer
- Vertraulichkeitsbezeichnung**: (empty field)
- Besitzer**: Keine Besitzer ausgewählt.
- Dynamische Mitglieder ***: (empty field)
- Dynamische Abfrage hinzufügen**: (link)

Bild 77: Gruppe definieren

Im Feld für die dynamische Abfrage klickst du rechts auf das **Stiftsymbol**, um den Regeleditor zu öffnen. Hier fügst du den dynamischen Abfragebefehl ein, der Geräte auf Basis ihres Zuweisungsprofils identifiziert. Als Beispiel könnte die Regel folgendermaßen lauten:

(device.devicePhysicalIds-any_-eq “[OrderID]:DE”)

Achte dabei darauf, dass der **Profilname** exakt mit dem Namen übereinstimmt, den du in der CSV-Zuordnung verwendet hast. Solltest du ein anderes Suffix wie z. B. -IT genutzt haben, passe den Namen entsprechend an. Nach dem Einfügen klickst du auf „**Speichern**“ und danach auf „**Erstellen**“, um die Gruppe endgültig zu erstellen.

Regelsyntax bearbeiten

Sie können Regeln schreiben und/oder direkt bearbeiten, indem Sie die Syntax im Feld unten bearbeiten. Beachten Sie, dass hier vorgenommene Änderungen möglicherweise nicht im Regel-Generator auf der linken Seite reflektiert werden.

Regelsyntax ⓘ

```
{device.devicePhysicalIds-any_-eq "[OrderID]:DE"}
```

Beispielregeln

```
(user.assignedPlans -all (assignedPlan.servicePlanId -eq "SCO")) -and (user.accountEnabled -eq true)  
(device.deviceOSType -eq "iPad") -or (device.deviceOSType -eq "AndroidForWork")
```

Bil 78: Regelsyntax bearbeiten

Sobald die Gruppe angelegt ist, kannst du sie über die Suchleiste wieder aufrufen und prüfen, ob sie bereits befüllt wurde. In der Gruppenübersicht siehst du ein Feld mit dem Erstellungsdatum sowie den Status der Verarbeitung. Theoretisch sollte die Zuweisung innerhalb von 60 Sekunden erfolgen. In der Praxis kann es jedoch zu deutlichen Verzögerungen kommen – manchmal dauert es mehrere Stunden, bis Geräte in der Gruppe erscheinen. Diese Verzögerung ist bekannt und lässt sich aktuell nicht zuverlässig umgehen.

Nach dem Anlegen der Gruppe erfolgt die Zuweisung eines bestehenden AutoPilot-Profil auf genau diese dynamische Gerätegruppe. Das Profil wird damit automatisch auf alle Geräte angewendet, die den definierten Gruppentag tragen. Dabei ist jedoch Geduld gefragt: Obwohl

Intune theoretisch alle 60 Sekunden die Gruppenmitgliedschaften aktualisieren sollte, kann die tatsächliche Verarbeitung in der Praxis deutlich länger dauern – teils bis zu mehreren Stunden.

Ein bekanntes Problem ist zudem, dass der in der CSV hinterlegte Gruppentag nicht sofort in Intune sichtbar wird. Es kann erforderlich sein, den Tag manuell im Intune Admin Center nachzutragen – unter Umständen mehrfach, da die Aktualisierung der Ansicht verzögert erfolgt. Erst wenn der Gruppentag korrekt erscheint, wird das Gerät auch durch die dynamische Regel der Gerätegruppe erfasst und dem Profil zugewiesen.

Besonders wichtig ist dabei die **Überprüfung des Profilstatus** im Geräteeintrag. Der Status muss auf *zugewiesen* stehen, bevor das Gerät per AutoPilot ausgerollt wird. Wird ein Gerät vor der erfolgreichen Zuweisung des Profils installiert, erfolgt kein kontrolliertes AutoPilot-Deployment – stattdessen verhält sich das Gerät wie ein herkömmlicher PC aus dem Einzelhandel.

Zugewiesenes Profil ⓘ
Nicht zugewiesen.
Zuweisungsdatum ⓘ
Nicht zugewiesen.
Registrierungsstatus ⓘ
Nicht angemeldet
Zugeordnetes Intune-Gerät ⓘ
N/V
Zugeordnetes Microsoft Entra-Gerät ⓘ
JVDST34
Zuletzt kontaktiert ⓘ
Nie
Bestellung ⓘ

Bild 79: Profilstatus

Wenn du mit Autopilot im Hybrid Join arbeitest, ist ein zusätzlicher Bestandteil erforderlich – der **Intune Connector for Active Directory**. Dieser Connector ist zwingend notwendig, um Geräte mit dem Hybrid Azure AD Join erfolgreich zu registrieren und bereitzustellen.

Zunächst solltest du prüfen, ob der Connector in deiner Intune-Umgebung bereits installiert wurde. Dies kannst du über das Microsoft Intune Admin Center unter „**Geräte**“ > „**Registrierung**“ > „**Intune Connector for Active Directory**“ nachvollziehen. Falls dort kein Eintrag vorhanden ist, steht dir die Option zur Verfügung, über „**Add**“ einen neuen Connector hinzuzufügen. Dabei handelt es sich um einen Agent, den du manuell herunterladen und auf einem Server deiner Wahl installieren musst.

Wähle für die Installation idealerweise einen Server aus, der sowohl eine Verbindung zum lokalen Active Directory als auch zum Internet besitzt. Geeignet sind beispielsweise Systeme in der DMZ oder Server, die über einen entsprechend konfigurierten Proxy Zugriff auf beide Seiten haben. Der Installationsprozess ist unkompliziert: Du führst das Setup auf dem Zielserver aus, klickst dich fünf- bis sechsmal durch den Assistenten mit „Weiter“ und schließt die Installation mit „Installieren“ ab. Weitergehende Konfigurationen sind in der Regel nicht notwendig.

Nach erfolgreicher Installation stellt der Connector sicher, dass Geräte über den Windows Autopilot-Prozess auch im hybriden Szenario korrekt in das lokale Active Directory aufgenommen werden. Du kannst damit also Geräte, die nicht rein cloudbasiert (Entra Joined) betrieben werden sollen, automatisiert provisionieren und mit der klassischen lokalen Infrastruktur verbinden.

Wenn du ausschließlich Cloud-only Deployments machst, also Geräte direkt über Entra Joined in die Cloud aufnimmst, ist der Intune Connector nicht notwendig. Im Fall von **hybriden Deployments** ist der Connector jedoch ein zwingender Bestandteil. Damit sind alle erforderlichen Komponenten für ein funktionierendes Hybrid Autopilot Deployment gegeben.

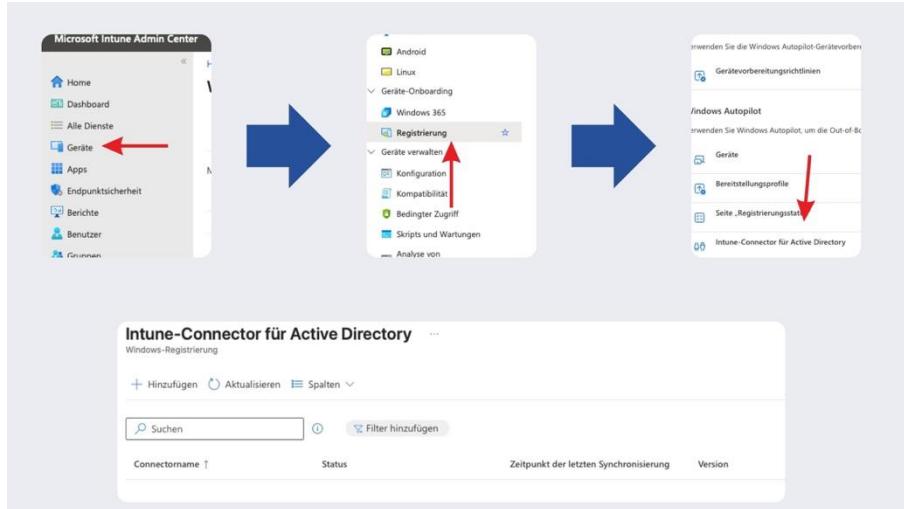


Bild 80: Intune Connector

Kapitel 16: Apple-Geräteverwaltung mit Intune und Apple Business Manager

Die Einbindung von Apple-Geräten in Microsoft Intune unterscheidet sich in mehreren Aspekten deutlich von der Windows-Geräteverwaltung. Im Mittelpunkt steht dabei die Entscheidung, ob ein Gerät über den **Apple Business Manager (ABM)** oder über den klassischen **BYOD-Weg (Bring Your Own Device)** mittels Unternehmensportal eingebunden wird. Diese Wahl hat direkte Auswirkungen auf die Steuerungsmöglichkeiten, den Automatisierungsgrad und die Richtliniendurchsetzung.

Im praktischen Einsatz zeigt sich häufig ein gemischtes Szenario. Bei einigen Unternehmen werden beispielsweise Geräte, die einem restiktiveren Management unterliegen sollen – etwa iPads für Auszubildende – über den **Apple Business Manager** eingebunden. Über diesen Weg lassen sich Geräte im sogenannten „Supervised Mode“ registrieren, wodurch eine umfassendere Steuerung möglich wird, z. B. die Unterdrückung des App Stores, die Blockierung von iCloud-Diensten oder das Setzen eines MDM-Löschschutzes.

Andere Geräte – wie etwa iPhones und iPads von Fachkräften in der Geschäftsleitung oder von Steuerberatern – werden dagegen bewusst **nicht über den Apple Business Manager**, sondern über das **Intune-Unternehmensportal** registriert. Diese Geräte befinden sich in der Regel im Besitz der Mitarbeitenden selbst oder sollen größere Freiheiten im Handling erlauben. Der

BYOD-Ansatz bringt allerdings auch Einschränkungen mit sich, etwa eine eingeschränkte Geräteüberwachung oder reduzierte Konfigurationsoptionen im Vergleich zur Supervised-Variante aus dem ABM.

Ein wesentliches Kriterium für die Entscheidung, welche Geräte über den ABM verwaltet werden und welche nicht, ist dabei oft das gewünschte Maß an Kontrolle. So entschied sich ein Unternehmen konkret dafür, die mobilen Endgeräte von Auszubildenden über den Apple Business Manager zu verwalten, um sie stärker einschränken zu können, während die dienstlichen Smartphones der Geschäftsleitung weniger restriktiv behandelt wurden und über das Unternehmensportal in Intune eingebunden sind. Der Apple Business Manager wurde in diesem Fall bewusst nicht für die Führungsebene genutzt, obwohl es technisch möglich gewesen wäre, alle Geräte darüber zu verwalten.

Diese Strategie zeigt exemplarisch, wie wichtig es ist, im Vorfeld eine **Zielgruppen-orientierte Geräteklassifizierung** vorzunehmen. Je nach Nutzergruppe, Einsatzzweck und Compliance-Anforderungen empfiehlt sich die Zuweisung unterschiedlicher Registrierungswege. Dabei spielt auch die Abwägung zwischen Verwaltungsaufwand, Nutzerfreundlichkeit und Sicherheitsanforderungen eine entscheidende Rolle.

Einbindung von Apple-Geräten, Zertifikatsverwaltung und Registrierungswege

Im Rahmen der Geräteeinbindung stellt sich häufig die Frage, wie Apple-Geräte sinnvoll in Microsoft Intune integriert werden können – insbesondere im Zusammenhang mit dem Apple Business Manager, dem Unternehmensportal und dem Gerätezertifikat.

Zunächst solltest du dir bewusst machen, dass die bloße Anlage von Apple IDs im Apple Business Manager nicht automatisch bedeutet, dass diese auch „geclaimt“ – also verwaltet – sind. Eine anschließende Prüfung ist daher essenziell. Sobald der Zugriff auf den Business Manager möglich ist, lässt sich leicht feststellen, welche Accounts tatsächlich beansprucht wurden. Das ist notwendig, da nur beanspruchte verwaltete Apple IDs vollständig unter Unternehmensverwaltung stehen und sich so für den Einsatz im User Enrollment eignen.

Ein häufiger Registrierungsweg – insbesondere in vielen Unternehmen und durch externe Dienstleister empfohlen – ist die Nutzung der **Unternehmensportal-App (Company Portal)** zur Registrierung. Zwar funktioniert dieser Weg technisch einwandfrei, er ist jedoch im Vergleich zu anderen Methoden weniger flexibel und bietet weniger granulare Steuerungsmöglichkeiten. Die Registrierung über das Unternehmensportal ist ein gängiges Szenario, wird jedoch zunehmend von eleganteren Verfahren abgelöst. Dennoch ist die bisherige Registrierung nicht obsolet – sie ist weiterhin gültig, wenngleich es modernere Alternativen gibt.

In vielen Fällen nutzen Unternehmen das Deployment über ein **MacBook**, auf dem ein entsprechendes Profil installiert wird. Der Apple Business Manager wird in solchen Fällen teilweise nur unterstützend verwendet. Probleme, wie langsames Laden von QR-Codes oder nicht übertragene Einstellungen, können in der Praxis auftreten. Diese Schwierigkeiten hängen möglicherweise mit der jeweiligen Konfiguration zusammen und sollten im Einzelfall überprüft werden.

Ein zentraler Bestandteil für die Registrierung von Apple-Geräten ist das **Apple Push-Zertifikat**. Dieses Zertifikat ist jeweils **365 Tage gültig** und muss rechtzeitig vor Ablauf verlängert werden.

Um das Zertifikat zu erstellen, gehst du folgendermaßen vor:

- **Geräte > Registrierung > Apple-MDM-Push-Zertifikat**
- **Du gehst die 5 Schritte durch**
- **Du lädst das Zertifikat hoch**



Bild 81: Apple Push Zertifikat beantragen

Das Zertifikat wird nicht automatisch erneuert – du musst es im Apple Push Certificates Portal **explizit verlängern**. Wenn du ein Apple Push-Zertifikat erneuern musst, ist es essenziell, dass du im **Apple Zertifikatsportal** nicht den Weg über eine **Neuanlage** gehst, sondern über den Pfad „**Renew**“ des bestehenden Zertifikats. Die Erneuerung betrifft ausschließlich das bereits vorhandene Zertifikat. Es darf **kein neues Zertifikat erstellt** werden.

Hintergrund ist, dass bei einer Neuanlage ein vollständig neuer Zertifikatsfingerabdruck generiert wird. Das bedeutet in der Praxis: **Geräte, die mit dem bisherigen Zertifikat verbunden waren, erkennen das neue Zertifikat nicht mehr**, nehmen keine Richtlinien mehr an und lassen sich nicht mehr verwalten. Gleichzeitig funktionieren neue Geräte nur noch mit dem neuen Zertifikat. Das führt zu einem Bruch im Deployment-Prozess und zwingt dich, dich für eine der beiden Seiten zu entscheiden – also entweder mit dem alten oder dem neuen Zertifikat weiterzuarbeiten. Im schlimmsten Fall müsstest du Geräte **neu registrieren**, was mit erheblichem Aufwand verbunden ist.

Das Verhalten unterscheidet sich deutlich von Google. Dort ist es im Kontext von **Android Enterprise** so, dass eine einmalige Registrierung genügt. Google prüft die Gültigkeit nicht erneut, und die Registrierung bleibt dauerhaft aktiv – ganz gleich, wie lange sie zurückliegt. Eine erneute Validierung entfällt komplett.

Bei Apple hingegen musst du regelmäßig nachweisen, dass du weiterhin autorisiert bist, Geräte über den Apple Business Manager und das Push-Zertifikat zu verwalten. Die Compliance-Anforderungen sind dort **deutlich strenger** und der Lifecycle eines Zertifikats ist auf **365 Tage** beschränkt. Spätestens vor Ablauf dieses Zeitraums musst du die **Erneuerung des bestehenden Zertifikats** durchführen, um Ausfälle in der Geräteverwaltung zu vermeiden.

Die Registrierung beim **Apple Business Manager** selbst ist mit erheblichem administrativem Aufwand verbunden. Du benötigst dafür unter anderem:

- Einen Handelsregisterauszug,
- eine D-U-N-S Nummer, die die Existenz deines Unternehmens bestätigt,
- und Geduld für die Validierungszeiten, die bis zu zwei Wochen und mehr in Anspruch nehmen können.

Im Gegensatz zu Google verlangt Apple bei jeder neuen Einrichtung des Business Managers eine umfassende Verifizierung, um sicherzustellen, dass der Antragsteller autorisiert ist. Diese Verfahren dienen der Sicherheit, erfordern jedoch organisatorisch und zeitlich eine gute Planung.

Zusätzlich solltest du bei der Verwaltung von Apple-Geräten auch den Punkt „**Bulk Enrollment Methods**“ im Blick haben. Hier findest du Plattform-Einstellungen sowie Registrierungsmethoden.

Übersicht zur Geräte-Registrierung über Enrollment Types (iOS/iPadOS)

Wenn du in Intune auf den Bereich **Enrollment Types** gehst, kannst du verschiedene Registrierungsarten für Apple-Geräte konfigurieren. In der aktuellen Umgebung wurde beispielsweise bereits die Geräte-Registrierung über das **Company Portal** eingerichtet – eine Methode, die du vielleicht ebenfalls verwendest. Das ist grundsätzlich kein schlechter Ansatz, war früher auch sehr gebräuchlich. Dennoch gibt es inzwischen weiterentwickelte, granulare Alternativen, die du kennen solltest.

Profile für Registrierungstyp

Apple-Registrierung

+ Profil erstellen ▾

Hiermit erstellen und verwalten Sie Registrierungstypprofile für iOS-/iPadOS-Benutzer mit privaten oder unternehmenseigenen Geräten. Diese Informationen

Priorität	Name	Beschreibung
1	iOS - User Choice	

Bild 82: Registrierungstypen

Unter iOS/iPadOS stehen dir drei Typen von Enrollment zur Verfügung. Insbesondere dann, wenn es sich **nicht** um Geräte handelt, die über den Apple Business Manager eingebunden werden, **nicht im Supervised-Modus** laufen oder **nicht zurückgesetzt** werden sollen, sind diese Optionen relevant. Dazu zählt:

- Web-based device enrollment (browserbasiert, ohne App)
- Account driven user enrollment
- Device enrollment with Company Portal (App-basiert)
- Device enrollment via Setup Assistant (DEP/Apple Business Manager)

In der Praxis empfehlen Microsoft und Apple zunehmend die erste Variante: **Web-based Enrollment**. Diese Methode ist insbesondere für Geräte ab **iOS 15** optimiert. Sie vermeidet die Notwendigkeit, die Company Portal App manuell zu installieren. Damit reduziert sich die Komplexität beim Onboarding deutlich – besonders hilfreich in **BYOD-Szenarien (Bring Your Own Device)**.

Beim web-basierten Enrollment handelt es sich um eine sogenannte **Just-in-Time-Registrierung**. Das bedeutet, der Nutzer muss nicht vorab die App installieren, sich anmelden und Zertifikate hinterlegen. Stattdessen wird ein Link verwendet, über den das Gerät direkt registriert werden kann. Du kannst die App später bei Bedarf trotzdem noch zuweisen.

Microsoft hat seine Dokumentation in diesem Zusammenhang kürzlich überarbeitet (z. B. „Overview of Apple device enrollment in Microsoft Intune“). Auffällig ist, dass das klassische

App-basierte Enrollment über das Company Portal dort **nicht mehr prominent aufgeführt** wird. Apple und Microsoft bewegen sich klar in Richtung webbasierter Registrierung.

Wichtig ist: Um diese Just-in-Time-Registrierung nutzen zu können, musst du folgende Voraussetzungen erfüllen:

- Die MDM-Autorität muss auf Intune gesetzt sein (ist durch die Intune-Lizenz abgedeckt).
- Ein gültiges Apple MDM Push-Zertifikat muss vorhanden sein (365 Tage gültig, jährliche Erneuerung notwendig).
- Es muss ein Enrollment-Profil in Intune erstellt werden, das mit den gewünschten Einstellungen konfiguriert ist.
- Es muss eine Just-in-time-Registrierung erstellt werden.

Diese Konfiguration bietet dir nicht nur eine moderne Benutzerführung, sondern auch mehr Flexibilität bei der Verwaltung von Apple-Geräten – insbesondere im nicht-supervised Bereich.

Webbasierte Registrierung von Apple-Geräten mit Intune (Just-in-Time Enrollment)

Die technische Einrichtung erfolgt über ein **Enrollment-Profil** in Intune sowie ein ergänzendes **Device Feature-Konfigurationsprofil** mit einem spezifischen Single Sign-On (SSO) Mechanismus. Das SSO-Profil basiert auf der Microsoft Entra ID und wird wie folgt konfiguriert:

- Devices > iOS/iPadOS > Configuration > Create new policy > Templates > Device Features

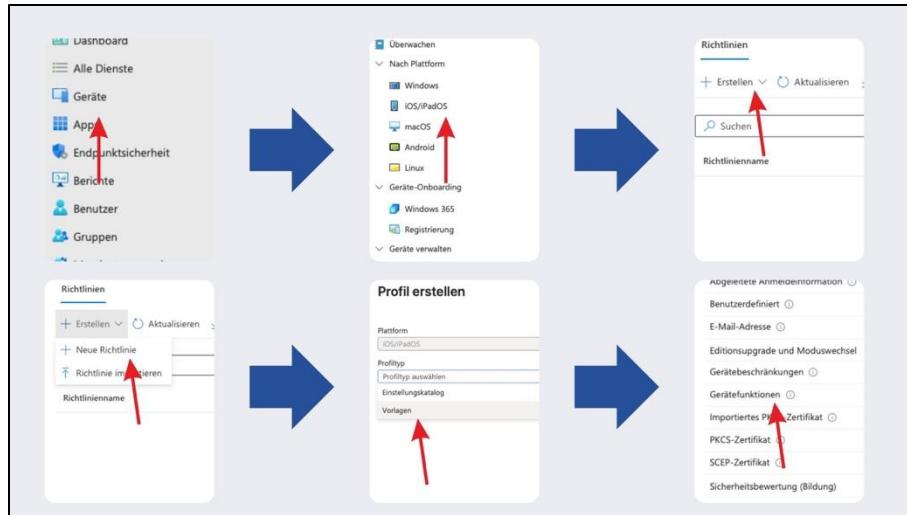
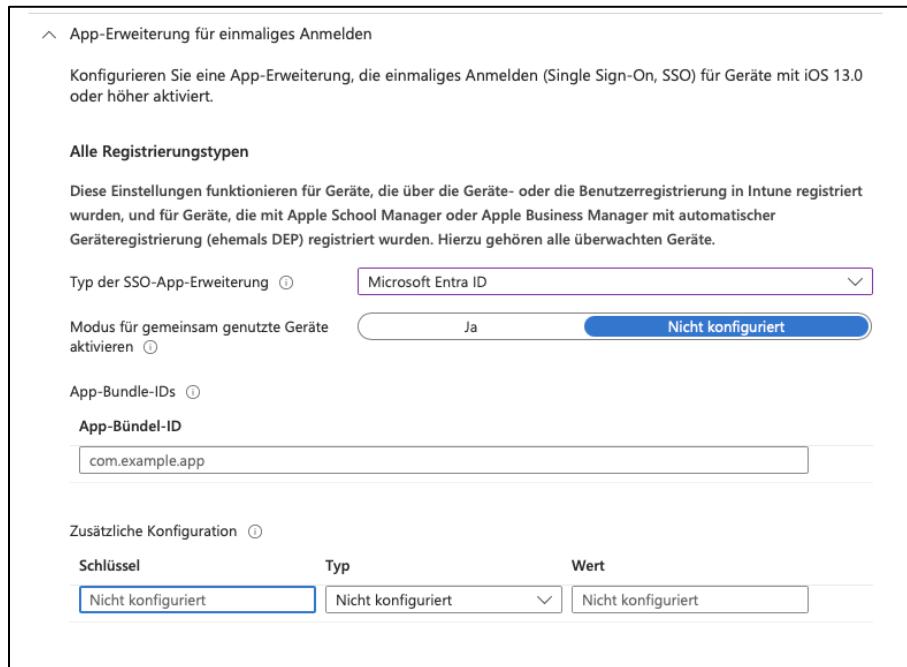


Bild 83: Just-in-time

- Profiltyp: Single Sign-On App Extension
- Extension Type: Microsoft Entra ID



The configuration page for the Microsoft Entra ID extension type:

- App-Erweiterung für einmaliges Anmelden:** Konfigurieren Sie eine App-Erweiterung, die einmaliges Anmelden (Single Sign-On, SSO) für Geräte mit iOS 13.0 oder höher aktiviert.
- Alle Registrierungstypen:** Diese Einstellungen funktionieren für Geräte, die über die Geräte- oder die Benutzerregistrierung in Intune registriert wurden, und für Geräte, die mit Apple School Manager oder Apple Business Manager mit automatischer Geräteregistrierung (ehemals DEP) registriert wurden. Hierzu gehören alle überwachten Geräte.
- Typ der SSO-App-Erweiterung:** Microsoft Entra ID (selected)
- Modus für gemeinsam genutzte Geräte aktivieren:** Ja (selected)
- App-Bundle-IDs:** com.example.app
- Zusätzliche Konfiguration:**

Schlüssel	Typ	Wert
Nicht konfiguriert	Nicht konfiguriert	Nicht konfiguriert

Bild 84: SSO

- Benötigte Schlüssel-Werte-Paare:
 1. Key: device_registration, Type: String Value: deviceRegistration
 2. Key: browser_sso_interaction_enable Type: Integer Value: 1

Zusätzliche Konfiguration ⓘ			
Schlüssel	Typ	Wert	
device_registration	Zeichenfolge	{{{DEVICEREGISTRATION}}}	 ...
browser_sso_interaction_enable	Ganze Zahl	1	 ...
Nicht konfiguriert	Nicht konfiguriert	Nicht konfiguriert	 ...

Bild 85: Schlüssel-Werte

Diese Konfiguration sorgt dafür, dass der SSO-Vorgang über den eingebauten Safari-Browser erfolgt und die Just-in-Time-Registrierung direkt mit Microsoft Entra ID interagiert.

Der webbasierte Weg erleichtert sowohl der IT als auch den Endanwendern den Registrierungsprozess. Er stellt sicher, dass alle erforderlichen Richtlinien und Einstellungen korrekt angewendet werden – und das mit einem minimalen Eingriff in die Geräte der Mitarbeitenden. Dieses Verfahren ist besonders dort sinnvoll, wo Geräte nicht über den ABM laufen und keine vollständige Kontrolle über das Gerät erforderlich ist.

Um das webbasierte Device Enrollment für iOS-Geräte in Intune effektiv einzusetzen, musst du die entsprechenden Profile gezielt zuweisen. Die Benutzer, deren Geräte über diese Methode registriert werden sollen, erhalten ein spezielles Enrollment-Profil. Für Benutzer, die bisher noch nicht damit arbeiten, kannst du ergänzend ein zweites Profil mit der alternativen Methode – etwa über das Company Portal – erstellen. Bei Bedarf kann der Wert in der Konfiguration jederzeit angepasst werden.

Die Registrierung selbst kann auf zwei Wegen ausgelöst werden:

- Wenn sich ein Benutzer mit seinem Geschäftskonto in einer geschäftlich genutzten App auf einem persönlichen Gerät anmeldet, wird die Registrierung automatisch initiiert.
- Alternativ kann dem Benutzer ein Registrierungslink übermittelt werden, etwa in der Form <https://portal.manage.microsoftenrollment.com>. Dieser kann auch maskiert, z. B. über TinyURL, bereitgestellt werden. Wird der Link über den Safari-Browser geöffnet, startet der Anmeldeprozess und das Gerät wird anschließend in Intune eingebunden.

Wurde das Enrollment erfolgreich abgeschlossen, kannst du über Intune entsprechende Richtlinien zuweisen. Diese werden unter **Device > Configuration > iOS/iPadOS > Device Restrictions** erstellt.

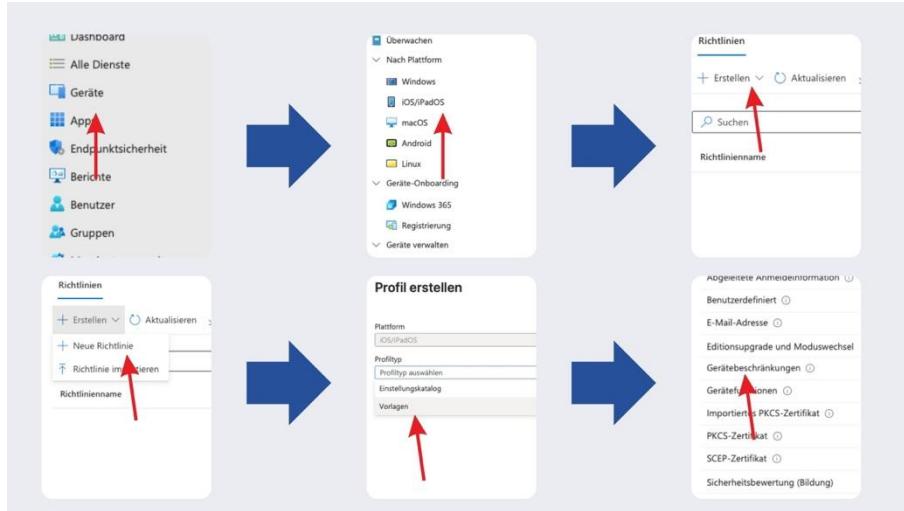


Bild 86: Device Restriction

Geräte, die über das Webbased Enrollment eingebunden wurden, erhalten ab diesem Punkt die volle Verwaltungskonfiguration. Geräte ohne ein passendes Profil hingegen erhalten nur einen eingeschränkten Funktionsumfang.

^ App Store, Dokumentanzeige, Spiele

Alle Registrierungstypen

Diese Einstellungen funktionieren für Geräte, die über die Geräte- oder die Benutzerregistrierung in Intune registriert wurden, und für Geräte, die mit Apple School Manager oder Apple Business Manager mit automatischer Geräteregistrierung (ehemals DEP) registriert wurden. Hierzu gehören alle überwachten Geräte.

Anzeige von Unternehmensdokumenten in nicht verwalteten Apps blockieren Ja Nicht konfiguriert

Lesen aus verwalteten Kontaktkonten für nicht verwaltete Apps zulassen Ja Nicht konfiguriert

AirDrop als nicht verwaltetes Ziel behandeln Ja Nicht konfiguriert

Anzeige nicht unternehmenseigener Dokumente in Unternehmens-Apps blockieren Ja Nicht konfiguriert

Zulassen, dass kopieren/einfügen durch verwaltetes Open-in betroffen ist Ja Nicht konfiguriert

Geräteregistrierung und automatische Geräteregistrierung

Diese Einstellungen funktionieren für Geräte, die über die Geräteregistrierung in Intune registriert wurden, und für Geräte, die mit Apple School Manager oder Apple Business Manager mit automatischer Geräteregistrierung (ehemals DEP) registriert wurden. Hierzu gehören alle überwachten Geräte.

iTunes Store-Kennwort für alle Käufe erforderlich Ja Nicht konfiguriert

In-App-Einkäufe blockieren Ja Nicht konfiguriert

Download von expliziten sexuellen Inhalten in Apple Books blockieren Ja Nicht konfiguriert

Schreiben von Kontakten in nicht verwaltete Kontaktkonten für verwaltete Apps zulassen Ja Nicht konfiguriert

Bild 87: Alle Registrierungstypen

Account Driven User Registrierung von Apple-Geräten

Neben dem webbasierten Verfahren bietet Intune auch **Account Driven User Enrollment**. Auch hierbei handelt es sich um ein BYOD-Szenario. Der entscheidende Unterschied besteht darin, dass geschäftliche und private Daten logisch voneinander getrennt gespeichert und verwaltet werden. Diese Trennung erfolgt durch Speicherung der Arbeitsdaten auf einem separaten Volume und durch Nutzung ausschließlich verwalteter Apps für Unternehmensdaten.

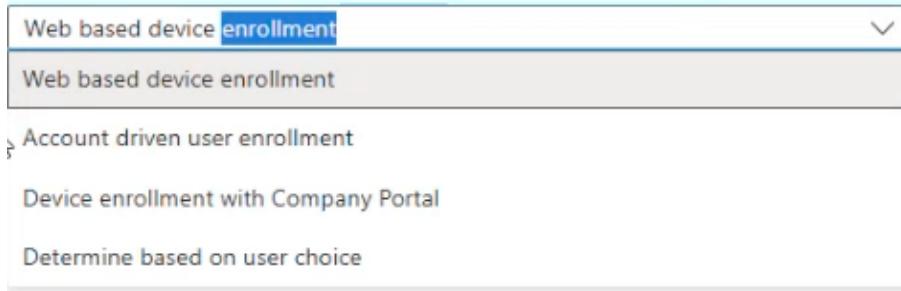


Bild 88: Account driven user enrollment

Für die Account Driven User Enrollment ist neben der MDM-Autorität und dem Apple MDM Push-Zertifikat zusätzlich eine **Managed Apple ID** erforderlich. Diese ist zwingend notwendig, um die Trennung zwischen privaten und geschäftlichen Inhalten zu gewährleisten. Ohne eine solche verwaltete Apple ID funktioniert dieses Verfahren nicht.

Der Unterschied liegt im Ablauf auf Seiten des Benutzers: Statt sich über einen Link zu registrieren, wie bei der webbasierten Variante, erfolgt die Anmeldung bei der Account Driven User Enrollment direkt über die Geräteeinstellungen, unter **VPN & Device Management** bei der sich der Benutzer in der iCloud mit der verwalteten Apple ID anmeldet. In beiden Fällen wird das Gerät automatisch mit dem MDM verbunden und unterliegt anschließend den vorgegebenen Richtlinien.

Im Rahmen der Apple-Geräteverwaltung in Intune ist insbesondere bei BYOD-Szenarien die Entscheidung über die Art der Datentrennung entscheidend. Wenn du eine saubere Trennung zwischen geschäftlichen und privaten Daten auf iOS-Geräten sicherstellen willst, ist das **Account Driven User Enrollment** der richtige Weg. Dabei wird auf dem Gerät eine optische und logische Trennung erzeugt: iCloud zeigt dem Benutzer sowohl einen *Personal Apple Account* als auch einen *Managed Apple Account* an. Diese klare Unterscheidung sorgt im Hintergrund für getrennte Volumes, Apps und Datenbereiche.

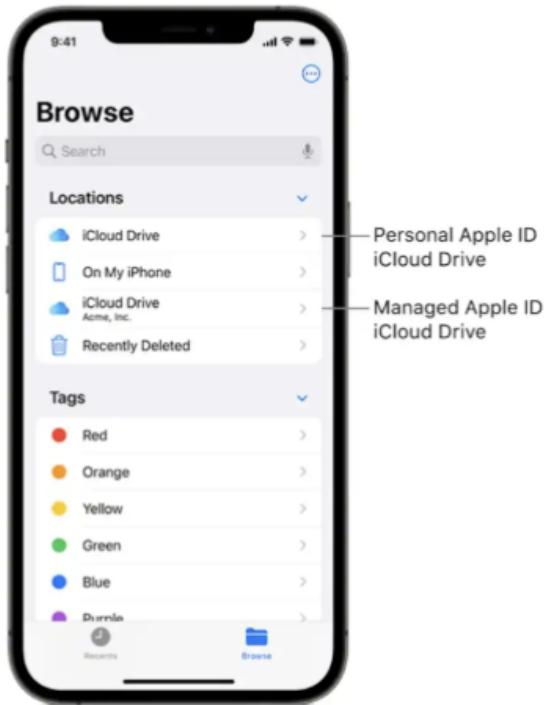


Bild 89: Trennung Apple ID's

Für Unternehmen, die BYOD ermöglichen, aber auf eine konsequente Trennung von Unternehmensdaten bestehen, ist diese Methode daher besonders geeignet. Eine zusätzliche Konfiguration wie „PublishFail“ ist heute nicht mehr notwendig – diese war nur in frühen Versionen der Lösung erforderlich und kann inzwischen vollständig ignoriert werden.

Eine alternative Konfiguration, bei der der Benutzer selbst zwischen geschäftlicher und privater Nutzung beim Enrollment wählen darf (beispielsweise über *UserChoice* oder *Term-Based* Optionen), wird nicht empfohlen. Diese Methode birgt ein hohes Fehlerpotenzial, da sie vom Nutzer technische Entscheidungen verlangt, die dieser häufig nicht zuverlässig treffen kann.

Falls ihr bisher keine **Managed Apple IDs** nutzt, müsstet ihr diese zwingend erstellen, um Account Driven Enrollment umsetzen zu können. Ohne verwaltete Apple ID ist diese Form der Trennung nicht möglich. In diesem Zusammenhang ist es auch wichtig zu wissen, dass die frühere Methode *Setup user enrollment with Company Portal* offiziell nicht mehr von Microsoft

Intune unterstützt wird. Diese Option gilt nur noch für bereits bestehende Geräte mit einem veralteten Profil und sollte zukünftig nicht mehr verwendet werden.

Ein weiterer Vorteil: Geräte müssen bei beiden Methoden **nicht zurückgesetzt** werden. Sie können im laufenden Betrieb integriert und verwaltet werden.

Kapitel 17: Verwaltung von Apple-Geräten mit dem Apple Business Manager und dem Enrollment Program Token

Im Rahmen der Geräteeinbindung über Apple bietet Intune zwei zentrale Mechanismen: den **Apple Configurator** und das **Enrollment Program Token** in Verbindung mit dem **Apple Business Manager**.



Bild 90: Methoden Massenregistrierung

Während der Apple Configurator häufig als Methode zur Massenbereitstellung beschrieben wird, handelt es sich hierbei nicht im eigentlichen Sinne um ein echtes "Bulk Enrollment", da jedes Gerät physisch angeschlossen, verbunden und initialisiert werden muss. Der Prozess ist zwar nicht kompliziert, aber mit manuellem Aufwand verbunden, da jedes Endgerät vor der Übergabe an den Nutzer einmal durch IT-Personal vorbereitet werden muss.

Effizienter ist die Verwendung des **Enrollment Program Token**, welches die direkte Integration des Apple Business Managers mit Intune erlaubt. Sobald ein Token konfiguriert wurde, synchronisieren sich automatisch alle im Apple Business Manager hinterlegten Geräte mit Intune. Diese Geräte erscheinen dann unter dem entsprechenden Token im Intune Admin

Center. Über diese Schnittstelle können Geräte vollständig automatisiert und ohne physischen Kontakt für die Verwaltung vorbereitet werden.

Wenn du im Intune Admin Center den Bereich *Devices > Enrollment > Apple Enrollment* aufrufst und dort in den Abschnitt *Enrollment Program Tokens* wechselst, kannst du einen bestehenden Token einsehen oder einen neuen erstellen. Klickst du auf „Create“, wird ein neuer Token erstellt und mit dem Apple Business Manager verknüpft. Nach erfolgreicher Einrichtung erscheinen in diesem Token-Bereich alle Geräte, die im Apple Business Manager registriert sind. Diese Geräte kannst du anschließend gezielt mit einem passenden Profil ausstatten.

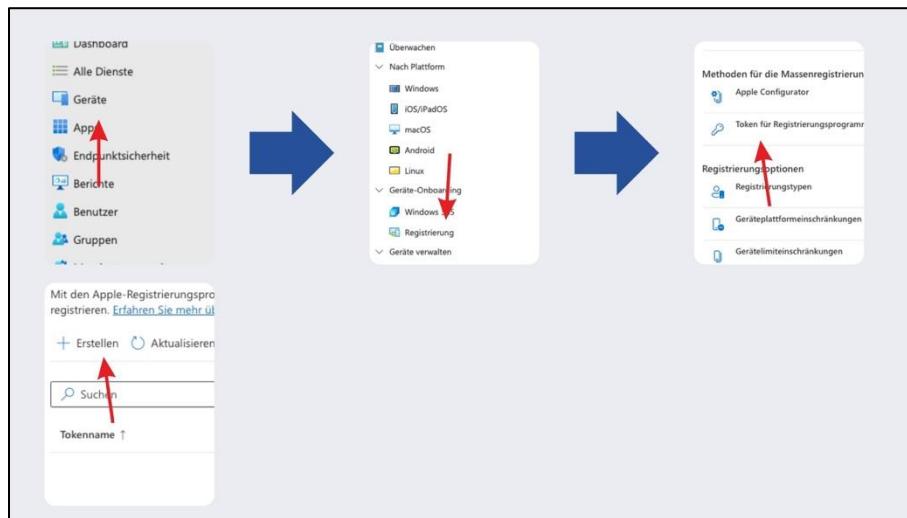


Bild 91: Token Enrollment

Token für Registrierungsprogramm hinzufügen

Token für Registrierungsprogramm

...

1 Grundlagen 2 Überprüfen + erstellen

* Ich erteile Microsoft die Erlaubnis, sowohl Benutzer- als auch Geräteinformationen an Apple zu senden. [Weitere Informationen](#)

Ich stimme zu.

* Laden Sie das Intune-Zertifikat mit öffentlichem Schlüssel herunter, das zum Erstellen des Tokens erforderlich ist.

Laden Sie Ihren öffentlichen Schlüssel herunter. 

Um Apple Business Manager zu nutzen, verwenden Sie Ihren Schlüssel, um ein Token über den unten angegebenen Link herunterzuladen.

[Token über Apple Business Manager erstellen](#) 

Oder

Um Apple School Manager zu nutzen, verwenden Sie Ihren Schlüssel, um ein Token über den angegebenen Link herunterzuladen. Für einige Features ist die Microsoft-Synchronisierung von Schul-/Unidaten erforderlich. [Weitere Informationen](#)

[Token über Apple School Manager erstellen](#) 

Speichern Sie die Apple-ID, die in Apple Business Manager oder Apple School Manager verwendet wird, um dieses Token zur späteren Referenz zu erstellen. Sie müssen sich beim Portal anmelden, um die Registrierungstoken jährlich zu erneuern.

Apple-ID *

Laden Sie Ihr Token hoch. Intune führt eine automatische Synchronisierung für Geräte aus Ihrem Apple Business Manager- oder Apple School Manager-Konto durch, das dem diesem Token zugeordneten MDM-Server zugewiesen ist.

Apple-Token

Bild 92: Grundlagen Token Registrierung

Im Unterbereich *Profiles* von einem Token kannst du für diese Geräte verschiedene Konfigurationsprofile anlegen. Bei der Erstellung eines neuen Profils für **iOS** oder **iPadOS** entscheidest du zunächst, ob das Gerät mit oder ohne Benutzerbindung (*User Affinity*) registriert werden soll. In typischen BYOD- oder persönlichen Nutzungsszenarien wählst du *Enroll with User Affinity*, während Geräte im KIOSK-Modus (*Shared Device*) ohne Benutzerbindung ausgerollt werden.

User Affinity & Authentication Method

User affinity *	Select an option
Management Options	Enroll with User Affinity <input checked="" type="radio"/> Enroll without User Affinity
Supervised	
Locked enrollment	Select an option
Sync with computers:	Select an option
Apple Configurator certificates:	Select certificate file to upload
Uploaded Certificates	
No certificates, select a certificate file to import.	

Bild 93: User affinity

Im Rahmen der Konfiguration eines Apple Enrollment-Profil im Intune-Portal gibt es verschiedene Einstellmöglichkeiten, die du abhängig vom Einsatzszenario sinnvoll aktivieren solltest. Eine dieser Einstellungen ist **Supervised**, den du auf „Ja“ setzen solltest. Dieser Modus erlaubt erweiterte Verwaltungsfunktionen auf dem Gerät und ist daher besonders für unternehmenseigene Geräte relevant.

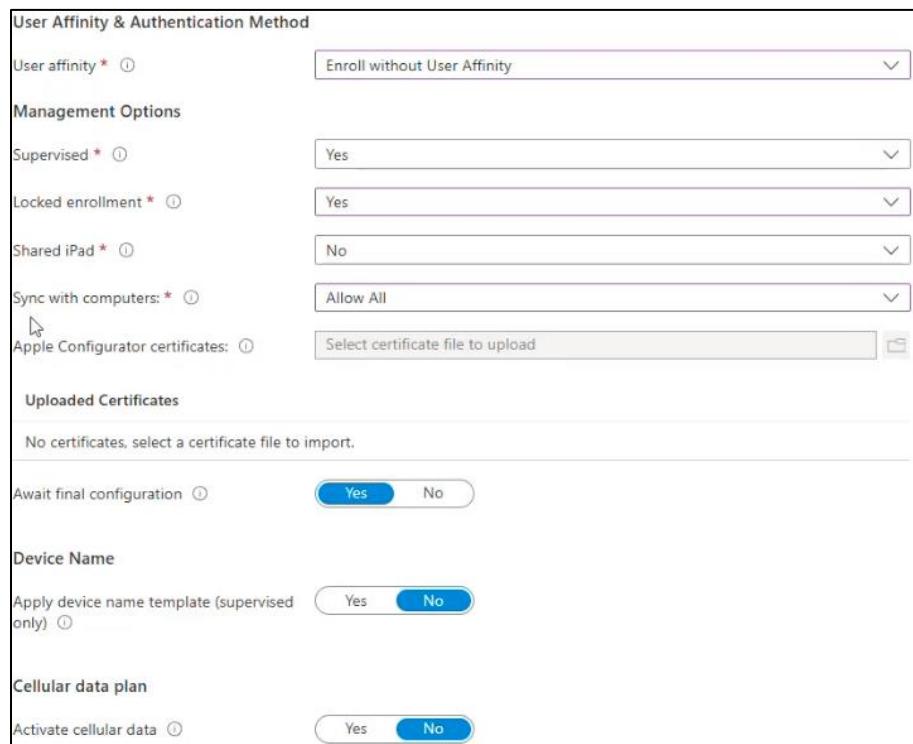
Auch die Einstellung **Shared iPad** kann bei Bedarf aktiviert werden – etwa, wenn mehrere Benutzer dasselbe iPad nutzen sollen. Diese Option unterscheidet sich in der Wirkung nicht wesentlich zwischen den verfügbaren Token-Typen, wie beispielsweise dem Microsoft Entra SharePoint. Beim Entra SharePoint wird zusätzlich automatisch der **Microsoft Authenticator** installiert. Hier solltest du abwägen, ob du diesen zwingend benötigst oder nicht.

Die Option **Sync with computers** ist in der Praxis bei etwa 90 % der Unternehmen aktiviert. Der Hintergrund: Es ist sehr aufwändig, Computernamen manuell in Zertifikate zu übertragen oder nachträglich zu ändern. Diese Methode gilt als eher veraltet, wird aber häufig beibehalten, weil bestehende Konfigurationen selten überarbeitet werden. Daher ist die Empfehlung, diese Option ebenfalls auf „Ja“ zu setzen.

Die Einstellung **Block device until all apps and profiles are installed** sorgt dafür, dass das Gerät erst nach vollständiger Installation aller Anwendungen und Richtlinien für den Benutzer freigegeben wird. Diese Option ist in den meisten Fällen sinnvoll und sollte ebenfalls aktiviert werden.

Ein weiterer Punkt ist **Apply Device Name Template**. Diese Einstellung erinnert in ihrer Funktion an das Autopilot-Profil für Windows. Du kannst hier ein Namensschema mit zwei Variablen – **Gerätetyp** und **Seriennummer** – definieren. Alternativ sind auch statische Werte möglich. In der Praxis bietet sich der Einsatz dieses Schemas an, auch wenn es in manchen Fällen deaktiviert ist. Die Entscheidung hängt von den jeweiligen Anforderungen ab.

Für Geräte mit **eSIM** oder **mobilien Datentarifen** kann die Einstellung **Cellular Data Plan** genutzt werden. Wenn du mit einem Mobilfunkanbieter zusammenarbeitest, der eSIM-Profilinformationen bereitstellt, kannst du hier eine entsprechende **URL** angeben. Diese wird beim Enrollment verwendet, um das Gerät mit einem Datenvertrag zu verbinden. Wenn du diese Funktion nicht nutzt, kannst du die Einstellung auf „Nein“ lassen.



The screenshot shows the 'User Affinity & Authentication Method' configuration page. It includes the following sections:

- User affinity ***: Set to "Enroll without User Affinity".
- Management Options**:
 - Supervised ***: Set to "Yes".
 - Locked enrollment ***: Set to "Yes".
 - Shared iPad ***: Set to "No".
 - Sync with computers: ***: Set to "Allow All".
 - Apple Configurator certificates:** A file upload field with a browse icon.
- Uploaded Certificates**: A note stating "No certificates, select a certificate file to import."
- Await final configuration**: A switch set to "Yes".
- Device Name**:
 - Apply device name template (supervised only)**: A switch set to "No".
- Cellular data plan**:
 - Activate cellular data**: A switch set to "No".

Bild 94: User Affinity & Authentication Method

Bei der Konfiguration von Apple-Geräten für den Unternehmenseinsatz im Intune-Portal lassen sich über das Registrierungsprofil gezielt verschiedene Elemente des Setup-Assistenten steuern. In der hier beschriebenen Konfiguration wurde das Profil zunächst auf Deutsch eingestellt. Die

Abteilung ist mit „IT“ angegeben, ebenso eine Rufnummer. Verschiedene Optionen sind sichtbar oder ausgeblendet – je nach gewünschter Benutzerführung während des Geräte-Onboardings:

Passcode	<input type="button" value="Hide"/> <input type="button" value="Show"/>	iMessage & FaceTime	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Location Services	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Onboarding	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Restore	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Screen Time	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Apple ID	<input type="button" value="Hide"/> <input type="button" value="Show"/>	SIM Setup	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Terms and conditions	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Software Update	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Touch ID and Face ID	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Watch Migration	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Apple Pay	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Appearance	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Zoom	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Device To Device Migration	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Siri	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Restore Completed	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Diagnostics Data	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Software Update Completed	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Display Tone	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Get Started	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Privacy	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Action button	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Android Migration	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Emergency SOS	<input type="button" value="Hide"/> <input type="button" value="Show"/>
Home Button	<input type="button" value="Hide"/> <input type="button" value="Show"/>	Terms of Address	<input type="button" value="Hide"/> <input type="button" value="Show"/>
		Intelligence	<input type="button" value="Hide"/> <input type="button" value="Show"/>

Bild 95: Setup-Assistent

- Ortungsdienste (Location Services): sichtbar
- Wiederherstellung (Restore): ausgeblendet
- Android-Migration: ausgeblendet
- Apple ID: ausgeblendet
- Terms and Conditions: ausgeblendet
- Touch ID und Face ID: sichtbar
- Apple Pay: ausgeblendet
- Zoom und Siri: ausgeblendet
- Diagnosedaten: ausgeblendet
- Display-Farbton, Home-Taste und Datenschutz: sichtbar
- iMessage & FaceTime: ausgeblendet
- Onboarding: sichtbar
- Bildschirmzeit und SIMs: ausgeblendet
- Softwareupdate: sichtbar
- Watch-Migration: ausgeblendet
- Darstellung (Appearance): sichtbar
- Migration von Gerät zu Gerät: sichtbar
- Wiederherstellung abgeschlossen: sichtbar
- Softwareupdate abgeschlossen: sichtbar

- Get started: ausgeblendet
- Action Button und Notfall-SOS: sichtbar
- Bedingungen der Adresse: ausgeblendet
- „Intelligenz“ (Apple Intelligence): sichtbar

Letzteres bezieht sich auf die neue Funktion „Apple Intelligence“, einen KI-gestützten Dienst von Apple. Bis vor Kurzem war diese Funktion in Europa durch die EU-Kommission untersagt. Eine aktualisierte Mitteilung von Apple datiert auf den 1. April 2025 bestätigt jedoch, dass „Apple Intelligence“ ab iOS Version 18.1 auch Käufern in Europa zur Verfügung stehen wird – insbesondere auf neuen Geräten wie dem iPhone 16.

In Unternehmen kann es daher sinnvoll sein, diese Funktion auf bereitgestellten Geräten zu deaktivieren, um unerwünschte Nutzung zu vermeiden. Insbesondere, da diese KI-Funktionalitäten wie Schreibunterstützung oder Notizoptimierungen mitbringen, die auf KI-Basis arbeiten, deren Integration bislang aus regulatorischen Gründen unterbunden war.

Wichtig: Die genannten Setup-Optionen lassen sich ausschließlich auf Geräten anwenden, die sich im **Apple Business Manager** befinden. Werden Geräte nicht über den Apple Business Manager verwaltet oder ohne diesen neu aufgesetzt, greifen die konfigurierten Einschränkungen nicht. Es ist jedoch möglich, ein Gerät im **Supervised Mode** zu betreiben, ohne es zwingend im Apple Business Manager zu registrieren – etwa durch die Nutzung entsprechender Registrierungsprofile. In diesen Fällen sind bestimmte Supervisor-Funktionen dennoch verfügbar, obwohl sie im Intune-Portal möglicherweise nicht sichtbar sind.

Die hier beschriebenen Konfigurationsprofile lassen sich zudem als **Standardprofile** für iOS-, iPadOS- oder macOS-Geräte definieren. Apple bietet in diesem Bereich mittlerweile vergleichbare Steuerungsmöglichkeiten wie Android – was in der Vergangenheit nicht immer gegeben war. Insbesondere für Registrierungs- und Setup-Optionen hat Apple deutlich aufgeholt.

Abschließend zur Frage der Benachrichtigung bei Ablauf des Zertifikats: Apple verschickt in der Regel eine entsprechende E-Mail. Allerdings kann dies in der Praxis auch einmal ausbleiben. Zusätzlich wird die Zertifikatsgültigkeit im Intune-Portal angezeigt. Um auf Nummer sicher zu gehen, empfiehlt es sich, eine eigene Erinnerung im Kalender zu setzen – eine Vorlaufzeit von

wenigen Tagen genügt in der Regel, da die Verlängerung des Zertifikats technisch nur wenige Minuten dauert.

Unabhängig von BYOD-Szenarien besteht zusätzlich die Möglichkeit, Geräte über den Apple Business Manager im sogenannten *Supervised Mode* zu verwalten. Dabei ist die zentrale Frage, ob die Geräte vor der Einbindung in Intune zurückgesetzt werden sollen oder nicht. Diese Entscheidung ist häufig weniger technischer Natur, sondern hängt vielmehr vom gewünschten administrativen Aufwand und der Bereitstellungsstrategie ab.

Eine Frage die zu den Einsatzmöglichkeiten aufkommt, ist der erläuterten Registrierungsmethoden im COP-Szenario (Corporate Owned, Personally Enabled) auf. Die vorgestellten Methoden sind primär für BYOD gedacht, finden jedoch auch gelegentlich in anderen Nutzungsszenarien Anwendung. Für den COP-Modus, insbesondere bei Android-Geräten, sei typischerweise die Registrierung über einen QR-Code vorgesehen. Wenn man im Apple-Kontext eine vergleichbare Lösung sucht, kommt das *Web-based Device Enrollment* in Kombination mit *App-Schutzrichtlinien* diesem Modell am nächsten. Intune selbst führt das COP-Szenario jedoch nicht als separates Konfigurationsprofil.

Kapitel 18: Verwaltung von Android-Geräten mit Intune – Registrierungsarten und Geräteeigentum

Zunächst navigierst du im Intune Admin Center in den Bereich **Devices** und dort weiter zu **Enrollment > Android**. Einer der ersten Schritte besteht darin, den **Managed Google Play Account** mit Intune zu verknüpfen.

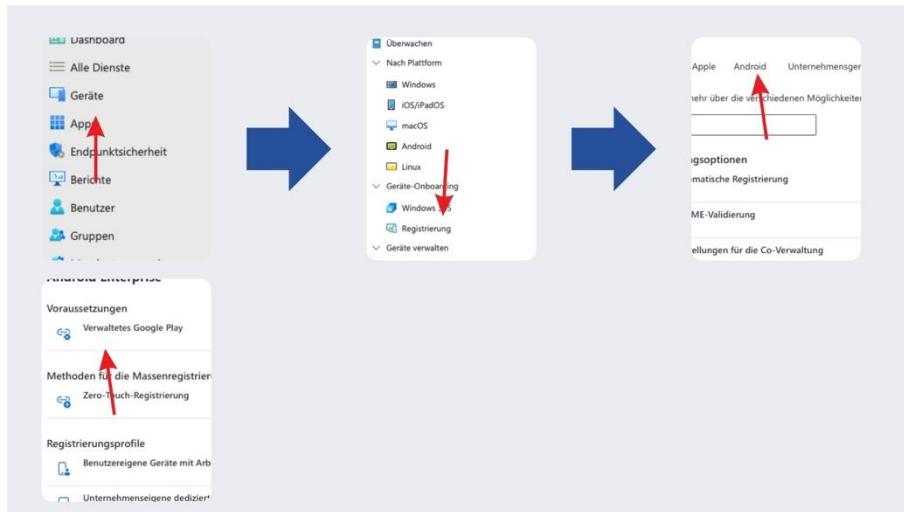


Bild 96: Managed Google Play einrichten

Diese Registrierung muss nur einmal durchgeführt werden. In der Benutzeroberfläche erkennst du die einmalige Einrichtung am angezeigten Datum. Eine erneute Anmeldung ist in der Regel nicht notwendig. Durch das einmalige Aktivieren dieses Dienstes bist du in der Lage, Android-Geräte über Intune zentral zu registrieren und zu verwalten.

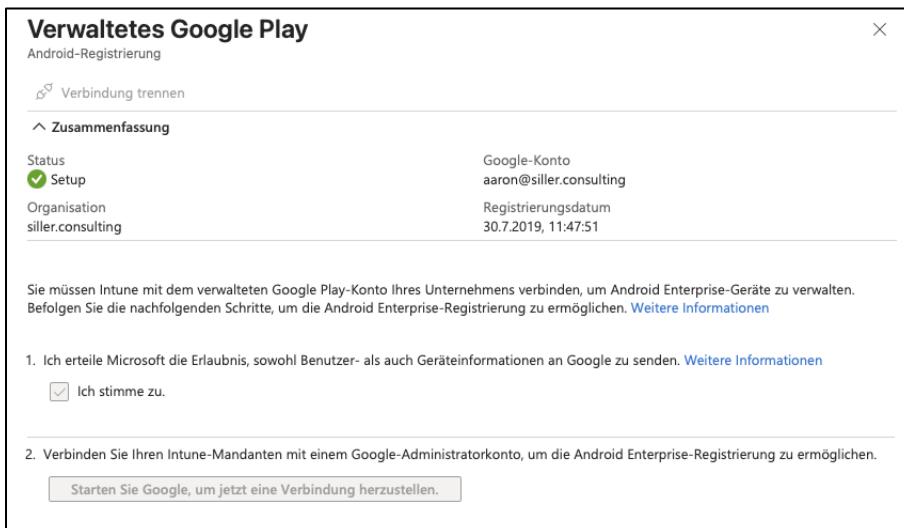


Bild 97: Managed Google Play

Sobald diese Verknüpfung aktiv ist, stehen dir unter Android mehrere Registrierungsarten zur Verfügung. Diese werden unter dem Punkt **Enrollment Profiles** verwaltet. Eine Besonderheit stellt dabei der Bereich **Android Open Source Project (AOSP)** dar. Dies ist nur dann relevant,

wenn du dedizierte Geräte verwalten möchtest, die ohne Google-Services wie den Play Store, Maps oder andere Google-Dienste betrieben werden. In den meisten Unternehmensumgebungen ist dieser Fall jedoch nicht gegeben, sodass diese Option in der Regel nicht verwendet wird.

Ein weiterer veralteter Registrierungsweg ist der **Android Device Administrator**. Dabei handelt es sich um eine frühere MDM-Plattform von Google, die heutzutage nicht mehr aktiv weiterentwickelt wird. Aus diesem Grund wird empfohlen, diesen Registrierungstyp über die Plattform-Einschränkungen in Intune zu blockieren, was du in einem früheren Kapitel bereits umgesetzt hast.

Android-Geräteverwaltung mit Intune – Enrollment-Typen und QR-Code-basierte Registrierung

Nachdem die Verknüpfung mit dem **Managed Google Play Store** erfolgt ist, kannst du unter **Devices > Android > Enrollment Profiles** verschiedene Profile für unternehmenseigene Geräte anlegen. Wenn du ein neues Profil für **Corporate-owned dedicated devices** erstellst, kannst du eine optionale Beschreibung vergeben und den **Token Type** auswählen.

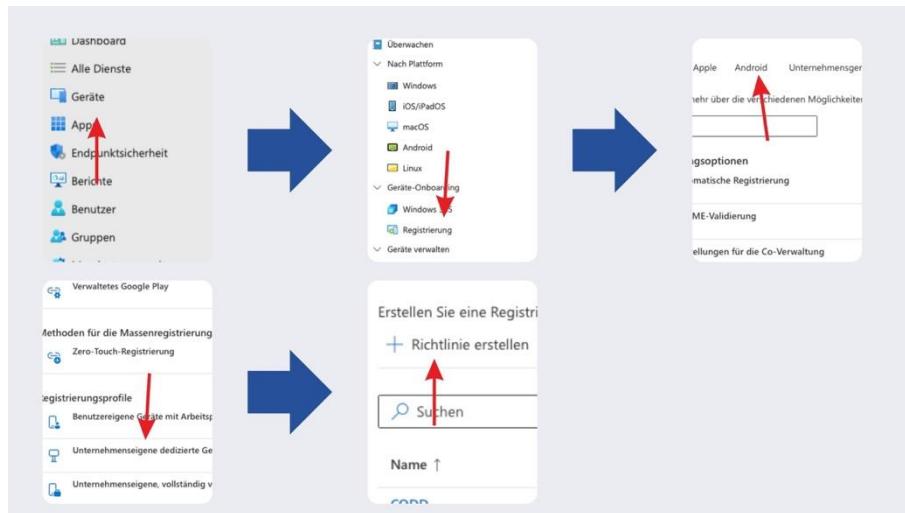


Bild 98: Android Enrollment Profiles

Hierbei stehen zwei Optionen zur Verfügung:

- Corporate-owned dedicated device (Default)
- Microsoft Entra Shared Device

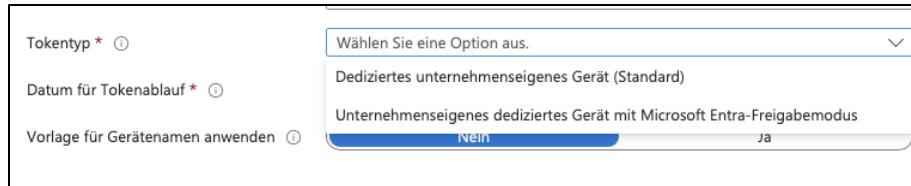


Bild 99: Tokentyp

Wenn du dich für den Microsoft Entra Shared Device Typ entscheidest, wird automatisch der Microsoft Authenticator mitinstalliert, sobald das Gerät registriert wird. Alternativ kannst du diesen auch nachträglich über Intune zuweisen.

Anschließend legst du das **Token Expiration Date** fest. Die maximale Gültigkeitsdauer beträgt 180 Tage. Nach dem Erstellen des Profils wird dir ein QR-Code angezeigt, den du für die Gerätebereitstellung nutzen kannst. Diesen findest du unter **Show Token**, zusammen mit einer Seriennummer.



Bild 100: QR-Code für Token

Für die Registrierung eines Geräts gehst du wie folgt vor:

1. Das Android-Gerät muss auf Werkseinstellungen zurückgesetzt sein.

2. Starte das Gerät.
3. An der Stelle, an der üblicherweise ein Google-Konto eingegeben wird, gibt es mehrere Möglichkeiten, den Registrierungsprozess zu starten:
 - Fünfmaliges Tippen auf eine freie Fläche des Bildschirms (öffnet die Kamera für den QR-Code-Scan).
 - Eingabe des Befehls `afw#setup`.
4. Nach dem Scannen des QR-Codes wird das Gerät automatisch als Corporate-owned dedicated device registriert.

Welches Profil verwendet wird, entscheidet der QR-Code. Über diesen Mechanismus kannst du auch Geräte mit anderen Besitztypen registrieren. Die folgenden Profiltypen stehen dir zusätzlich zur Verfügung:

1. Corporate-owned Fully Managed User Devices

Dieses Profil ist nahezu identisch im Setup wie das „Dedicated“-Profil. Auch hier erhältst du einen QR-Code, der auf Werkzustand zurückgesetzte Geräte in den Android Enterprise-Modus versetzt. Sobald der Code gescannt ist, erfolgt die Registrierung als vollständig verwaltetes unternehmenseigenes Gerät. Intune weist diesem Gerät dann Richtlinien und Applikationen zentral zu. Beachte, dass diese Geräte laut Microsoft ausschließlich für den geschäftlichen Gebrauch vorgesehen sind – auch wenn manche Unternehmen sie in der Praxis für gemischte Nutzung freigeben.

2. Corporate-owned Devices with Work Profile

Dieses Profil kombiniert das Konzept von Unternehmensbesitz mit einem getrennten Arbeitsbereich, ähnlich wie bei BYOD-Geräten. Auch hier wird ein QR-Code generiert, mit dem du das Gerät registrierst. Der Hauptunterschied besteht darin, dass der private und der geschäftliche Bereich auf dem Gerät strikt getrennt sind. Die Optik und Handhabung dieser Trennung hängt von der Android-Version und vom Gerätehersteller ab – teilweise wird lediglich ein separater Ordner angezeigt, in anderen Fällen lässt sich zwischen „Privat“ und „Arbeit“ per Schaltfläche wechseln.

Ein wichtiger Aspekt aller QR-Code-basierten Enrollment-Methoden ist der Geräte-Reset: Du musst das Gerät auf Werkseinstellungen zurücksetzen, bevor du es in Intune integrieren kannst.

Für viele Unternehmen ist dies ein erheblicher Aufwand, insbesondere bei Bestandsgeräten. Aus diesem Grund greifen manche lieber auf die BYOD-Variante zurück, bei der ein Reset nicht notwendig ist.

In der Android-Geräteverwaltung mit Intune gibt es unterschiedliche Ansätze, die je nach Geräteeigentum, Einsatzzweck und administrativem Aufwand gewählt werden können. Entscheidest du dich für ein vollständig verwaltetes Gerät, also ein **Fully Managed Device**, befinden sich alle Geräteeinstellungen vollständig unter Kontrolle der IT. Die Richtlinien greifen in diesem Fall systemweit, und du kannst nahezu jede Konfiguration technisch durchsetzen.

Anders ist es bei der Nutzung eines privaten Geräts mit Arbeitsprofil (**BYOD mit Work Profile**). In diesem Szenario wird lediglich ein abgeschotteter Arbeitsbereich auf dem Gerät bereitgestellt. Nur innerhalb dieses Bereichs wirken die zugewiesenen Richtlinien. Sobald sich der Benutzer außerhalb des Arbeitsbereichs bewegt, greifen die Konfigurationen und Einschränkungen nicht mehr. Das bedeutet, dass du als Administrator nur begrenzten Einfluss auf den privaten Teil des Geräts hast.

Eine flexible Zwischenform stellt das sogenannte **COP (Corporate-Owned, Personally Enabled)**-Modell dar. Dabei handelt es sich um ein unternehmenseigenes Gerät, das sowohl dienstlich als auch privat genutzt werden kann. Technisch ist es ein vollständig verwaltetes Gerät, das aber zusätzlich zur Nutzung für private Zwecke freigegeben wird. Du kannst damit sowohl systemweite als auch profilbezogene Richtlinien durchsetzen. Gleichzeitig eröffnet dir das COP-Modell die Möglichkeit, mit **App-Schutzrichtlinien (App Protection Policies)** zu arbeiten. Diese erlauben es, Applikationen wie Outlook, Word oder Teams in eine Art Container zu verlagern, in dem zusätzliche Sicherheitsregeln – etwa zur Datenübertragung, Zwischenablage oder Speicherort – greifen. Diese Schutzrichtlinien sind jedoch eher optional und sollten erst dann umgesetzt werden, wenn die Gerätebereitstellung als solche stabil und zuverlässig funktioniert.

Ein weiteres wichtiges Thema im Kontext der Android-Geräteverwaltung ist **Android Zero-Touch Enrollment**. Dabei handelt es sich um eine vergleichbare Lösung zum **Apple Business Manager**, mit dem Geräte automatisiert und ohne manuelle Eingriffe bereitgestellt werden können. Zero-Touch funktioniert nur, wenn du über einen autorisierten Reseller verfügst, der deine Geräte im Portal registriert. Dies kann beispielsweise Samsung Knox sein. Anders als beim Apple Business

Manager erfordert Zero-Touch in der Praxis jedoch etwas mehr manuelle Eingaben. Die Integration in Intune verläuft nicht ganz so reibungslos, ist aber technisch stabil.

Methoden für die Massenregistrierung



Zero-Touch-Registrierung

Bild 101: Zero-Touch-Registrierung

Bei der Wahl des richtigen Enrollment-Typs – ob BYOD, COP, Fully Managed oder Dedicated Device – solltest du auch einen Blick auf die verfügbaren **Geräteeinschränkungsrichtlinien (Device Restrictions)** werfen. Je nach Typ unterscheidet sich der Umfang der konfigurierbaren Optionen erheblich.

Wenn du zum Beispiel in Intune eine neue Gerätekonfigurationsrichtlinie unter **Devices > Configuration > Android Enterprise**. Nun hast du zwei Bereiche: Einmal **Fully Managed, Dedicated, and Corporate-Owend Work Profile** und einmal den Bereich **Personally-Owend Work Profile**. Gehe unter dem Bereich **Fully Managed, Dedicated, and Corporate-Owend Work Profile** auf **Device Restrictions** gehst, stehen dir deutlich mehr Optionen zur Verfügung als im BYOD-Szenario. Unter dem Abschnitt „General“ kannst du unter anderem folgende Einstellungen blockieren:

- Datum- und Uhrzeiteinstellungen ändern
- USB-Datentransfer
- Bluetooth-Konfiguration
- Bildschirmaufnahmen
- Factory Reset
- Zugriff auf USB-Speichergeräte

Vollständig verwaltete, dedizierte und unternehmenseigene Arbeitsprofilgeräte

Diese Einstellungen funktionieren für vollständig verwaltete, dedizierte und unternehmenseigene Arbeitsprofilgeräte.

Bildschirmaufnahme (Arbeitsprofilebene)	Blockieren	Nicht konfiguriert
Kamera (Arbeitsprofilebene)	Blockieren	Nicht konfiguriert
Standardberechtigungsrichtlinie (Arbeitsprofilebene)	Gerätestandard	▼
Datums- und Uhrzeitänderungen	Blockieren	Nicht konfiguriert
Roamingdatendienste	Blockieren	Nicht konfiguriert
Konfiguration des WLAN-Zugriffspunkts	Blockieren	Nicht konfiguriert
Bluetooth-Konfiguration	Blockieren	Nicht konfiguriert
Tethering und Zugriff auf Hotspots	Blockieren	Nicht konfiguriert
USB-Dateübertragung	Blockieren	Nicht konfiguriert
Externe Medien	Blockieren	Nicht konfiguriert
Daten mithilfe von NFC (Arbeitsprofilebene) übertragen	Blockieren	Nicht konfiguriert
Entwicklereinstellungen	Erteilen Sie	Nicht konfiguriert
Mikrofonanpassung	Blockieren	Nicht konfiguriert
E-Mail-Adressen für Schutz vor Zurücksetzung auf Werkseinstellungen	Nicht konfiguriert	▼
Systemupdate	Gerätestandard	▼
Sperrzeiträume für Systemupdates	Importieren	Exportieren

Bild 102: Vollständig verwaltete Geräte

Einige Funktionen stehen zudem exklusiv im KIOSK-Modus zur Verfügung.

Vollständig verwaltete und dedizierte Geräte (nur Kioskmodus)

Diese Einstellungen funktionieren nur für vollständig verwaltete und dedizierte Geräte, die mit einer Kioskrichtlinie betrieben werden.

Menü für Einschalttaste	Blockieren	Nicht konfiguriert
Warnungen bei Systemfehlern	Erteilen Sie	Nicht konfiguriert
Aktivierte Systemnavigationsfeatures	Nicht konfiguriert	▼
Systembenachrichtigungen und -informationen	Nicht konfiguriert	▼
Endbenutzerzugriff auf Geräteeinstellungen	Blockieren	Nicht konfiguriert

Bild 103: Funktionen KIOSK-Modus

Im Vergleich dazu bietet das BYOD-Profil (Personal Owned with Work Profile) deutlich weniger Möglichkeiten. Auch hier kannst du Geräte-Einschränkungen setzen, aber nur innerhalb des Arbeitsprofils. Beispielsweise kannst du:

- Copy & Paste zwischen Arbeits- und Privatbereich blockieren
- Bildschirmaufnahmen unterbinden
- Zugriff auf Kamera oder Kontakte steuern
- Passwortanforderungen definieren



Bild 104: Allgemeine Einstellungen BYOD

Ein vergleichbares Verhalten findest du übrigens auch im iOS-Bereich. Wenn du hier beispielsweise eine neue Richtlinie unter **iOS/iPadOS > Device Restrictions** erstellst und etwa die Synchronisierung von iCloud-Fotos deaktivieren möchtest, dann funktioniert das nur bei Geräten, die über **Device Enrollment** oder **Automated Device Enrollment** eingebunden wurden. BYOD-Geräte unter iOS bieten hier ebenfalls nur eingeschränkte Steuerungsmöglichkeiten.

Geräteregistrierung und automatische Geräteregistrierung

Diese Einstellungen funktionieren für Geräte, die über die Geräteregistrierung in Intune registriert wurden, und für Geräte, die mit Apple School Manager oder Apple Business Manager mit automatischer Geräteregistrierung (ehemals DEP) registriert wurden. Hierzu gehören alle überwachten Geräte.

Synchronisierung von Fotos mit iCloud blockieren ⓘ	Ja	Nicht konfiguriert
iCloud-Fotomediathek blockieren ⓘ	Ja	Nicht konfiguriert
"Mein Fotostream" blockieren ⓘ	Ja	Nicht konfiguriert
Übergabe blockieren ⓘ	Ja	Nicht konfiguriert

Bild 105: Device Restriction iOS/iPadOS

Die Entscheidung für oder gegen ein bestimmtes Enrollment-Szenario hängt also stark davon ab, wie viel Kontrolle du auf das Gerät ausüben willst, wie hoch der Aufwand für die Bereitstellung sein darf und welche Anforderungen deine Organisation an Datenschutz und Nutzungsfreiheit stellt.

Kapitel 19: Namenskonventionen, Domain Join und Geräteeigentum im Windows Autopilot Hybrid Join

Im Rahmen der Konfiguration von Autopilot Hybrid Join in Microsoft Intune spielt das Festlegen eines Computernamens sowie der Ziel-Domäne eine zentrale Rolle. Diese Einstellungen nimmst du im Intune Admin Center unter **Konfiguration > Windows 10 and later** mit dem Template **Domain Join** vor.

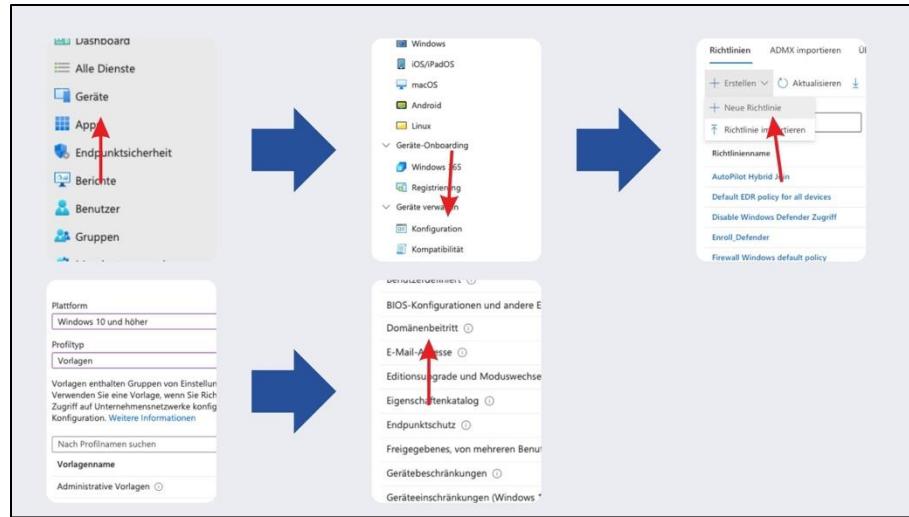


Bild 106: Hybrid Joined

Sobald du ein entsprechendes Profil anlegst, findest du dort die Option *Computer Name Prefix*. Mit diesem Präfix kannst du einen festen Namensbestandteil vorgeben, beispielsweise „SillerConsulting-“. Intune ergänzt diesen automatisch auf bis zu 15 Zeichen, indem eine zufällige Zeichenkombination aus Groß- und Kleinbuchstaben sowie Zahlen generiert wird. Der resultierende Gerätename entspricht optisch häufig nicht den unternehmensüblichen Namenskonventionen. Unternehmen, die Wert auf standardisierte oder nachvollziehbare Namen legen – z. B. durch Seriennummern oder Standortbezüge – empfinden diese Zufallsnamen oft als unpassend.

Im selben Profil gibst du unter *Domain Name* die Ziel-Domäne an, der das Gerät beitreten soll. Optional kann auch eine dedizierte Organisationseinheit (OU) hinterlegt werden. Wird keine OU definiert, erfolgt der Join automatisch in die Standard-OU „Computers“.



Bild 107: Konfigurationseinstellungen

An einem Beispiel lässt sich veranschaulichen, wie ein solcher Gerätename aussieht, wenn er durch die Zufallsgenerierung vervollständigt wird. Das entspricht der Standardfunktionalität, sobald keine andere Namenslogik über zusätzliche Mechanismen implementiert wird. Es ist auch möglich, den Join-Typ eines Geräts im Nachgang zu ändern – etwa von einem Microsoft Entra Joined Gerät zu einem Hybrid Joined Gerät. Derartige Änderungen können je nach Unternehmensstruktur und technischen Anforderungen notwendig sein.

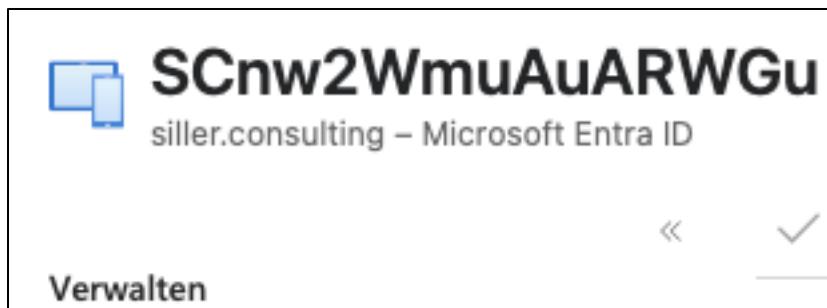


Bild 108: Beispiel Namensgenerierung

Darüber hinaus kannst du in Intune die Eigenschaft *Device Ownership* eines Geräts manuell ändern. Dies ist insbesondere relevant, wenn Geräte zunächst als persönliche Geräte registriert wurden und im Nachgang als unternehmenseigene Geräte klassifiziert werden sollen. In der Praxis wird dies direkt über die Eigenschaften des Geräts unter **Devices > Properties** umgesetzt. Einige Funktionen – beispielsweise die korrekte Auflistung installierter Anwendungen – funktionierten erst nach dieser Anpassung zuverlässig. Rein funktional ergibt sich durch die Änderung des Eigentumsstatus jedoch keine Erweiterung der Rechte; entscheidend für Richtlinien und Zugriffsmöglichkeiten bleibt weiterhin der ursprüngliche Registrierungsweg des Geräts.

Neben der Eigentumszuordnung kannst du auch mit **Device Categories** arbeiten. Diese Funktion findest du im Intune Admin Center unter **Devices**, dort im unteren Bereich. Über den Button *Create* legst du eigene Gerätekategorien an. Die Kategoriennamen kannst du frei wählen – etwa nach Standort, Abteilung oder Gerätetyp. Diese Kategorien eignen sich insbesondere als Filterkriterium in dynamischen Gruppen, über die du gezielt Richtlinien oder Applikationen zuweisen kannst.

Auch der Eigentumsstatus eines Geräts – also ob „Personal“ oder „Company“ – kann als Filterkriterium für dynamische Gruppen verwendet werden. Dies bietet dir eine zusätzliche Möglichkeit, Konfigurationen und App-Zuweisungen strukturiert und zielgerichtet umzusetzen. Auf diese Weise lässt sich Intune noch präziser in bestehende IT-Strukturen einbinden.

Kapitel 20: Verwaltung von Apple IDs und Domainerfassung im Apple Business Manager

Manager

Für die Integration von Apple-Geräten in Microsoft Intune und insbesondere für das *User Enrollment* mit einer klaren Trennung zwischen privaten und geschäftlichen Daten, ist der Einsatz verwalteter Apple-IDs im **Apple Business Manager (ABM)** erforderlich. Wenn du im ABM arbeitest, siehst du unter dem Bereich „Benutzer“ die verwalteten Apple-Accounts deiner Organisation. Diese kann nicht im privaten App Store verwendet werden, da sie ausschließlich für den geschäftlichen Kontext vorgesehen ist.

Unternehmen verfolgen hier unterschiedliche Ansätze. Eine Variante ist es, die geschäftliche Domäne vollständig für verwaltete Apple-IDs zu reservieren. Alternativ kann die gleiche Domäne auch für private Apple-IDs verwendet werden, was jedoch zu Konflikten führen kann. Im Apple Business Manager kannst du unter **Einstellungen > verwaltete Apple-Accounts** einsehen, ob und wie deine Domäne dort bereits konfiguriert ist.

Es ist eine grundlegende Konfiguration vorhanden, jedoch ohne aktivierte **Verzeichnissynchronisierung**. Diese Funktion ermöglicht es, alle Microsoft Entra ID-Konten automatisch mit dem Apple Business Manager zu synchronisieren. Gleichzeitig kann es dabei zu Konflikten kommen – etwa dann, wenn bereits Apple-IDs mit derselben Domäne privat registriert wurden. In einem konkreten Fall wurden 33 Benutzernamen als „conflicted“ angezeigt, obwohl nur 11 bereits verwaltet waren. Diese Konflikte kannst du über die Funktion **Verwalten** auflösen.

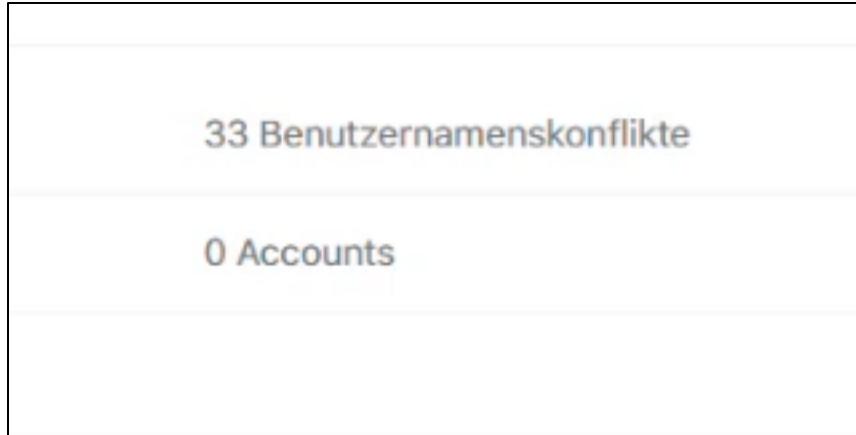


Bild 109: 33 Benutzernamenskonflikte

Ein zentraler Schritt in der vollständigen Verwaltung ist die **Domainerfassung**. Diese findest du ebenfalls unter den Einstellungen. Mit dem Start der Domainerfassung erklärst du, dass die Domain deiner Organisation exklusiv verwaltet wird. Bestehende private Apple-IDs unter dieser Domain werden dadurch identifiziert und es wird ein Übertragungsverfahren eingeleitet. Betroffene Benutzer erhalten eine E-Mail mit dem Hinweis, dass ihre Apple-ID nun verwaltet wird. Sie haben ab Erhalt 30 Tage Zeit, sich darauf einzustellen; nach dieser Frist greifen erste Einschränkungen. Technisch betrachtet sind es sogar 60 Tage, bis die Verwaltung vollständig umgesetzt wird. Mit Abschluss dieser Maßnahme ist es nicht mehr möglich, weitere private Apple-IDs mit dieser Domain zu erstellen.

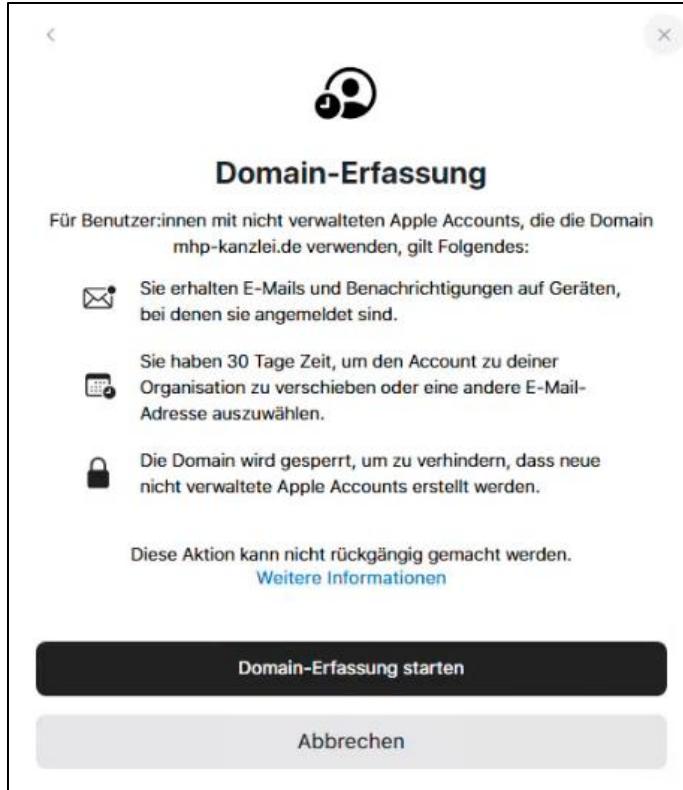


Bild 110: Domain-Erfassung

Verwaltete Apple-IDs sind Voraussetzung für das *User Enrollment* im sogenannten Account-driven Szenario. Nur so lässt sich die klare Trennung zwischen geschäftlichen und privaten Daten auf Apple-Geräten technisch realisieren. Du solltest die betroffenen Nutzer im Vorfeld klar und rechtzeitig informieren – idealerweise mit einem Hinweis auf den genauen Zeitplan, die kommenden Schritte und den Inhalt der automatisierten Apple-Benachrichtigung. Bei unternehmensweiten Umstellungen – etwa bei mehreren hundert oder tausend betroffenen Konten – ist dies unerlässlich, um Rückfragen oder Störungen im laufenden Betrieb zu minimieren.

In kleineren Umgebungen ist der organisatorische Aufwand überschaubar. Dennoch bleibt die Kommunikation an die Nutzer entscheidend, da die Apple-ID nicht mehr für den privaten App Store genutzt werden kann.

Die entscheidende Frage ist, wie gut die Benutzer mit dem Vorgang der Apple-ID-Erstellung und der Umstellung auf eine verwaltete Apple-ID umgehen können. Während der Prozess für

technisch versierte Anwender in der Regel problemlos umsetzbar ist, zeigen sich insbesondere im geschäftlichen Umfeld häufig Unsicherheiten, die zu Rückfragen führen. Um das zu vermeiden, empfiehlt sich eine strukturierte Begleitung des Prozesses.

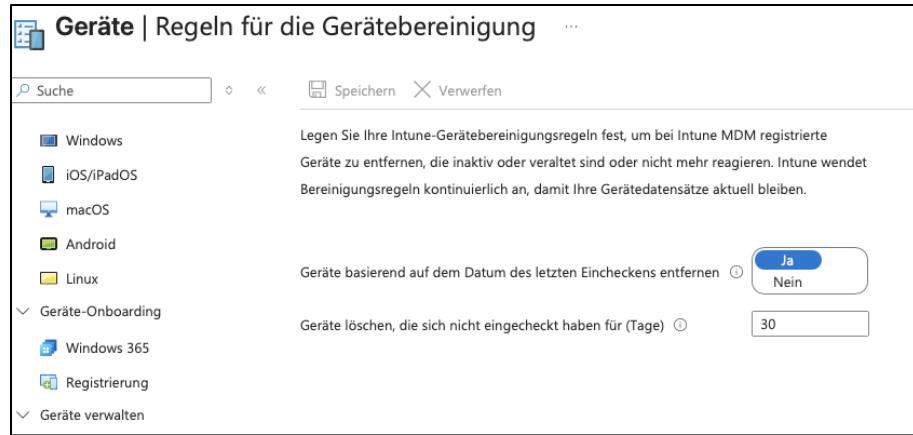
Falls du bereits einen **MDM-Server-Token** hinterlegt hast und deine Geräte mit dem Apple Business Manager synchronisiert werden, stellt die Domainerfassung und Einführung verwalteter Apple-IDs den nächsten logischen Schritt dar, wenn du mit *User Enrollment* oder der allgemeinen Trennung von geschäftlicher und privater Nutzung arbeiten wollt.

Einige Unternehmen entscheiden sich dafür, die Einführung verwalteter Apple-IDs und die damit verbundene Domainerfassung im Apple Business Manager schrittweise umzusetzen. In solchen Fällen ist es üblich, zunächst zu analysieren, welche Benutzerkonten betroffen sind – insbesondere, ob es sich bei diesen Accounts um aktive Mitarbeitende handelt oder um ehemalige Beschäftigte, die bereits aus dem Unternehmen ausgeschieden sind. Häufig wird abgewartet, bis sich die Zahl der betroffenen Nutzer reduziert hat. Sobald eine überschaubare Menge an Konten übrig bleibt, wird dann zu einem definierten Zeitpunkt die Domainerfassung durchgeführt und die verbliebenen Konten werden übernommen oder gesperrt.

Dieses Vorgehen ist organisatorisch sinnvoll, da sich technische Änderungen an Apple-IDs direkt auf die Endnutzer auswirken. Auch wenn die technische Umsetzung selbst nicht besonders komplex ist, ist der unmittelbare Einfluss auf den Arbeitsalltag der Nutzer nicht zu unterschätzen. Deshalb empfiehlt es sich, alle beteiligten Benutzer frühzeitig zu informieren und in den Prozess einzubeziehen, um Akzeptanz und Verständnis für die Maßnahme zu schaffen.

Kapitel 21: Gerätebereinigung und Compliance-Richtlinien in Microsoft Intune

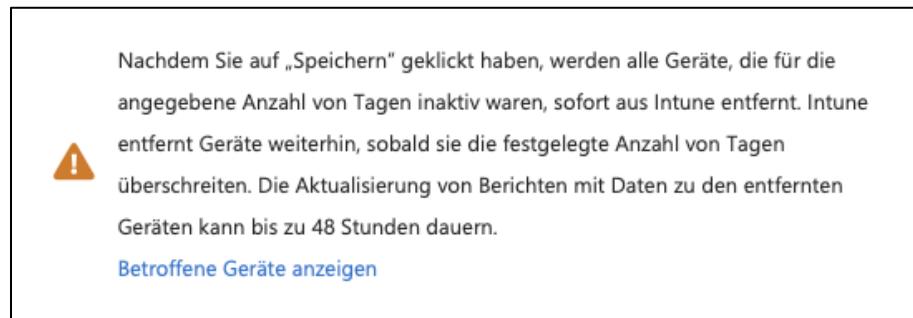
Im Intune Admin Center steht dir unter **Devices > Device clean-up rules** eine wichtige Funktion zur Verfügung, mit der du nicht mehr verwendete oder lange nicht mehr synchronisierte Geräte automatisiert bereinigen kannst. Diese Bereinigungsfunktion solltest du aktivieren, sofern dies noch nicht geschehen ist. Ein häufig genutzter Schwellenwert liegt bei **90 Tagen**, in vielen Umgebungen sind jedoch auch **30 oder 45 Tage** praktikabel.



The screenshot shows the 'Geräte | Regeln für die Gerätbereinigung' (Devices | Rules for device cleanup) page. On the left, there's a sidebar with icons for Windows, iOS/iPadOS, macOS, Android, and Linux. Below that are sections for 'Geräte-Onboarding' (Windows 365, Registrierung) and 'Geräte verwalten'. At the top right, there are 'Speichern' (Save) and 'Verwerfen' (Discard) buttons. A main text area says: 'Legen Sie Ihre Intune-Gerätbereinigungsregeln fest, um bei Intune MDM registrierte Geräte zu entfernen, die inaktiv oder veraltet sind oder nicht mehr reagieren. Intunewendet Bereinigungsregeln kontinuierlich an, damit Ihre Gerätedatensätze aktuell bleiben.' Below this, there are two buttons: 'Ja' (Yes) and 'Nein' (No), with 'Ja' being highlighted. Another section below says: 'Geräte löschen, die sich nicht eingecheckt haben für (Tage)' with a input field set to '30'.

Bild 111: Device clean-up-rule

Wenn du in die Einstellung gehst und beispielsweise „30 Tage“ auswählst, kannst du über den Link **View affected devices** alle Geräte anzeigen lassen, die sich in diesem Zeitraum nicht mit Intune synchronisiert haben. Solche Geräte werden dann automatisch aus dem Intune-Verzeichnis entfernt. Das bringt insbesondere im Zusammenhang mit **Conditional Access Policies** oder **App-Schutzrichtlinien** Vorteile, da du sicherstellen kannst, dass nur verwaltete und aktive Geräte auf Unternehmensressourcen zugreifen können.



Nachdem Sie auf „Speichern“ geklickt haben, werden alle Geräte, die für die angegebene Anzahl von Tagen inaktiv waren, sofort aus Intune entfernt. Intune entfernt Geräte weiterhin, sobald sie die festgelegte Anzahl von Tagen überschreiten. Die Aktualisierung von Berichten mit Daten zu den entfernten Geräten kann bis zu 48 Stunden dauern.

Betroffene Geräte anzeigen

Bild 112: Betroffene Geräte anzeigen

Die Bereinigung greift außerdem in Situationen, in denen das **Offboording von Geräten** nicht sauber durchgeführt wurde – etwa wenn ein Mitarbeitender das Unternehmen verlässt und das Gerät zwar zurückgibt, aber nicht vollständig aus dem Intune-Asset-Management entfernt wird. Auch gestohlene oder verlorene Geräte, die sich nicht mehr melden, können auf diese Weise automatisch entfernt werden.

Wichtig zu wissen ist, dass sich die **Device Clean-up Rules** ausschließlich auf die letzte erfolgreiche Synchronisierung beziehen. Ob ein Gerät als „compliant“ oder „non-compliant“ gekennzeichnet ist, spielt für die Clean-up-Logik keine Rolle.

Um die Compliance im Unternehmen zu überwachen, solltest du dir zusätzlich die Konformitätseinstellungen im Bereich **Devices > Compliance** ansehen. Hier gibt es eine Einstellung namens „**Mark devices with no compliance policy assigned as**“, die du auf „**Not compliant**“ setzen solltest. Hintergrund: Intune weist jedem registrierten Gerät standardmäßig eine sogenannte **Default Device Compliance Policy** zu. Diese enthält jedoch keine sinnvollen Prüfungen, sondern dient lediglich dazu, das Gerät nicht als vollständig „unbekannt“ zu führen.



Bild 113: Nicht konform

Die Empfehlung lautet daher, **eigene Compliance-Richtlinien zu erstellen**, die echte Anforderungen überprüfen. Gehe dazu auf **Create Policy**, wähle deine Plattform (z. B. Windows 10/11), und konfiguriere in den folgenden Schritten konkrete Prüfungen, etwa:

- Device Properties: z. B. Mindestversion von Windows 11 (etwa Windows 11 H2).
- Device Health: z. B. Microsoft Defender aktiv und aktueller Bedrohungsstatus.
- System Security: z. B. BitLocker muss aktiviert sein, Passwortvorgaben müssen erfüllt sein.
- Microsoft Defender for Endpoint Integration: Mindestbewertung der Gerätesicherheit.

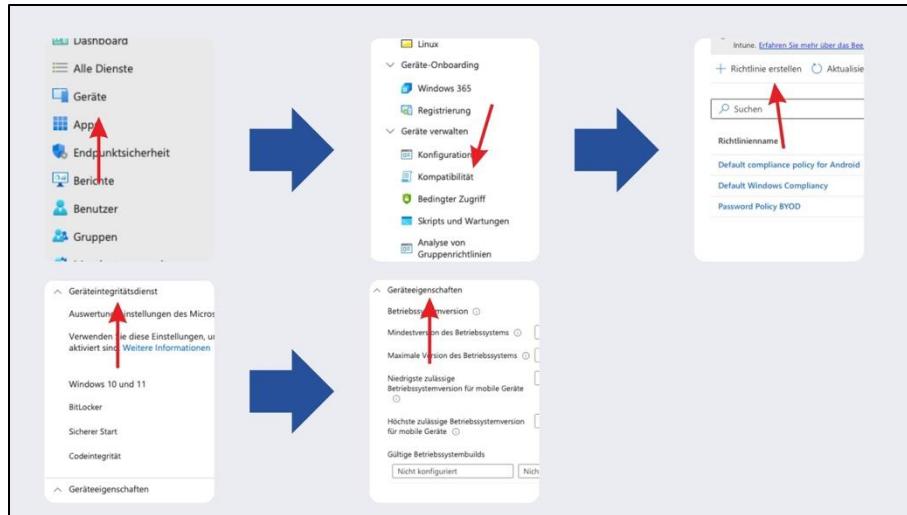


Bild 114: Compliance Richtlinie

Diese Richtlinien weist du anschließend gezielt einer oder mehreren Benutzer- oder Gerätegruppen zu.

Die vollen Kontrollmöglichkeiten entfalten diese Richtlinien im Zusammenspiel mit **Conditional Access Policies** in **Microsoft Entra ID**. Erst durch diese Kombination kannst du den Zugriff auf Ressourcen wie Exchange Online, SharePoint oder Teams unterbinden, wenn ein Gerät nicht den definierten Sicherheitsanforderungen entspricht.

Innerhalb der Compliance-Definitionen gibt es zusätzlich den Bereich **Actions for non compliance**. Hier kannst du z. B. festlegen, ob Benutzer bei Verstoß gegen Richtlinien benachrichtigt werden sollen. Die Option „**Send email to end user**“ ist allerdings mit Vorsicht zu genießen. Eine generische Benachrichtigung darüber kann schnell zu Missverständnissen führen, insbesondere wenn die Benutzer nicht wissen, was sie konkret unternehmen sollen. In der Praxis reicht es meist aus, Geräte als „**Not compliant**“ zu kennzeichnen, ohne eine automatische Nachricht zu versenden.

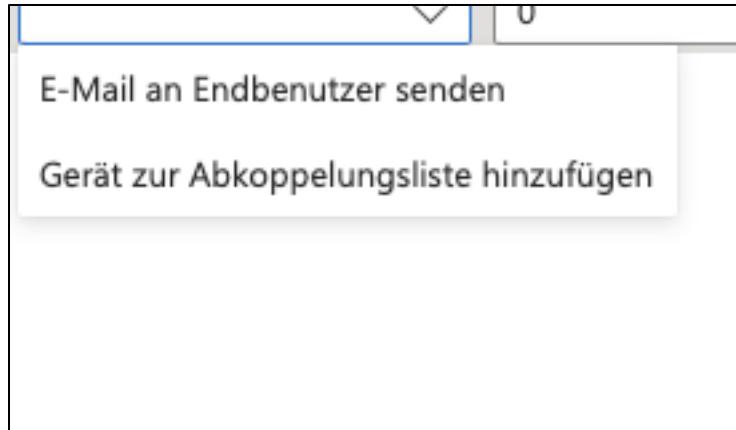


Bild 115: E-Mail an Benutzer

Ein bekanntes Problem in Intune ist, dass das **Reporting** teilweise ungenau sein kann. Geräte springen mitunter zwischen den Zuständen „compliant“, „non-compliant“ oder „not evaluated“, was die Übersicht erschwert. Auch deshalb ist es sinnvoll, eigene Richtlinien mit klaren Prüfregeln zu verwenden und nicht auf die Default-Logik zu vertrauen.

Du hast zudem die Möglichkeit, über **PowerShell-Skripte** zusätzliche Prüfungen durchzuführen, etwa wenn du sehr spezifische Anforderungen oder Geräteauswertungen umsetzen willst, die mit den Standardrichtlinien nicht abbildbar sind. In den meisten Fällen reichen jedoch die grafisch konfigurierbaren Compliance-Richtlinien aus.

In Intune kann es zu einem bekannten Anzeigefehler kommen, wenn du mit benutzerdefinierten Konformitätsrichtlinien arbeitest und gleichzeitig die **Default Device Compliance Policy** aktiv ist. Du kannst dies wie folgt nachvollziehen: Navigiere zu einem registrierten iOS-Gerät und öffne dort unter **Gerätekompatibilität** die Standardrichtlinie. Es kann vorkommen, dass diese Richtlinie mit einem roten „X“ als *nicht konform* markiert ist. Dies steht im Widerspruch zur eigentlich gültigen, benutzerdefinierten Konformitätsrichtlinie, die korrekt zugewiesen und erfüllt ist.

Dieser Widerspruch ist ein **Bug im Intune-Backend**, bei dem die Überschreibung der Default Policy durch eine eigene Richtlinie nicht korrekt dargestellt wird. Funktional hat dies jedoch keine Auswirkungen, sofern du mit eigenen Richtlinien arbeitest – die Standardrichtlinie wird

dabei tatsächlich **überschrieben**. Die fälschliche Darstellung kann ignoriert werden, solange keine zusätzliche Bewertung durch Conditional Access Policies daran gekoppelt ist.

Ein Workaround für dieses Anzeigeproblem besteht darin, die eigene Richtlinie **kurzzeitig zu entfernen und erneut zuzuweisen** sowie das betroffene Gerät zu synchronisieren. Alternativ kannst du die **Default Device Compliance Policy vollständig deaktivieren**, wenn du sicherstellst, dass alle betroffenen Geräte durch eigene Richtlinien abgedeckt sind. Das Deaktivieren dieser Default Policy triggert ebenfalls eine neue Systemsynchronisation, was zur Korrektur der fehlerhaften Anzeige führen kann.

Beachte jedoch, dass bei der erstmaligen Deaktivierung der Standardrichtlinie **alle Geräte im System temporär als „nicht konform“ angezeigt werden**. Dieser Zustand normalisiert sich in der Regel nach der nächsten erfolgreichen Synchronisierung der Richtlinien. Entscheidend ist dabei: **Solange keine Conditional Access Policies mit dem Konformitätsstatus verknüpft sind**, entstehen daraus keine funktionalen Einschränkungen.

Wenn du diesen Weg wählst, solltest du die betroffenen Geräte und Richtlinien kurzzeitig im Blick behalten und sicherstellen, dass alle benutzerdefinierten Konformitätsrichtlinien korrekt greifen. Nur so kannst du gewährleisten, dass deine Geräte nicht unbeabsichtigt als non-compliant deklariert werden und dadurch etwa der Zugriff auf Ressourcen blockiert wird.

Kapitel 22: Einführung in Conditional Access – Grundlagen und empfohlene Richtlinien

Conditional Access (CA) stellt eines der leistungsfähigsten Sicherheitsinstrumente in Microsoft Entra ID dar. Es ermöglicht dir, granulare Zugriffssteuerungen für Benutzer und Geräte zu definieren, um Unternehmensressourcen abzusichern. Trotz seiner Bedeutung zeigt eine Statistik einer Sicherheitskonferenz, dass etwa 70 % der Microsoft-365-Tenants in Deutschland Conditional Access nicht oder nur sehr eingeschränkt nutzen. Dabei ist es gerade in Kombination mit Intune und anderen Sicherheitsfunktionen eines der zentralen Werkzeuge für Zero-Trust-Strategien.

Wenn du in das Intune-Portal wechselst und unter „**Conditional Access**“ den Punkt „**Policies**“ aufrufst, findest du eine Übersicht aller vorhandenen Richtlinien. Eine klare und strukturierte **Namenskonvention** ist hier essenziell. Unklare Bezeichnungen wie „Block Internal“ helfen im täglichen Betrieb nicht weiter. Empfehlenswert ist, die Richtlinien z. B. mit einer Kennzahl zu beginnen, gefolgt von einer klaren Beschreibung, wie z. B. CA001_AI-
IUsers_RequireCompliantDevice.

Richtliniename	Tags	Status	Warnung
Multifactor authentication for admins accessing Microsoft Admin Portal	VON MICROSOFT VERWALTE	Ein	
Multifactor authentication for per-user multifactor authentication users.	VON MICROSOFT VERWALTE	Ein	
Allow Germany/Poland		Nur melden	

Bild 116: Conditional Access

Die typischen Bestandteile einer Richtlinie sind:

- Zielgruppen (Users): Für Zuweisungen solltest du entweder mit All Users arbeiten und bestimmte Benutzer gezielt excluden, oder mit einer gut gepflegten dynamischen Gruppe. Einzelne Benutzer oder statische Gruppen solltest du vermeiden, da hierbei sehr leicht Benutzer übersehen werden.
- Ausnahmen (Exclusions): Du solltest immer einen Break-Glass-Account definieren, also ein Notfallkonto mit globalen Administratorrechten und keinerlei Richtlinieneinschränkungen. Dieses Konto sollte nur in Notfällen verwendet werden und gut abgesichert sein.

Ein weiterer zentraler Punkt bei Conditional Access ist die Auswahl der **geschützten Ressourcen**. Microsoft empfiehlt eine sogenannte „**any-any**“-Policy, die sämtliche Benutzer und Ressourcen umfasst und grundlegende Sicherheitsanforderungen durchsetzt. Eine weitere elementare Ressourcengruppe, die du absichern solltest, ist die **Office 365 Suite** (Exchange, SharePoint, Teams, etc.).

Als erste Maßnahme empfiehlt es sich zu prüfen, ob Zugriffe auf Unternehmensdaten über unsichere Pfade wie öffentlich erreichbare Apps oder Endgeräte ohne Schutzmechanismen möglich sind. Du kannst etwa mit CA sicherstellen, dass:

- Datenzugriffe nur von konformen Geräten erfolgen dürfen.
- Geräte hybrid joined oder Entra joined sein müssen.

- Der Zugriff nur nach erfolgreicher MFA erlaubt ist.
- Bestimmte Länder oder IP-Bereiche vom Zugriff ausgeschlossen sind.

Wechsle dazu in eine neue Richtlinie (**New Policy**) und wähle zunächst unter **Assignments → Users** alle Benutzer (All Users) aus, exkludiere ggf. Admins oder Testnutzer. Danach bestimmst du unter **Cloud Apps or Actions** z. B. die gesamte **Office 365 Suite** als Ziel.

Unter **Access controls → Grant** konfigurierst du, dass der Zugriff nur erlaubt ist, wenn das Gerät als **konform markiert** ist (*Require device to be marked as compliant*). Alternativ kannst du mehrere Bedingungen kombinieren, wie etwa:

- Require hybrid Azure AD joined device
- Require MFA

Diese Bedingungen können wahlweise mit **AND** oder **OR** verknüpft werden.

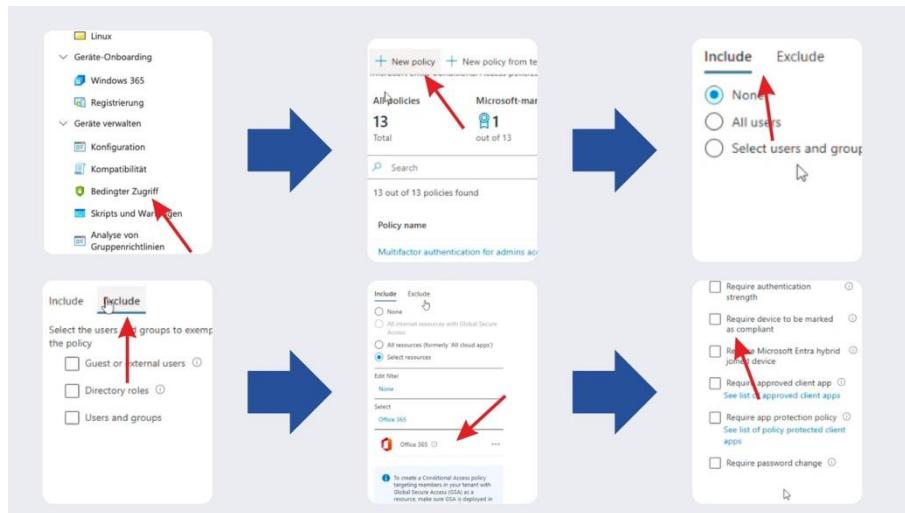


Bild 117: Conditional Access

Ein Hinweis zur Manipulationssicherheit: Es gibt Methoden, mit denen sich der Compliance-Status eines Geräts theoretisch fälschen lässt. Dies ist technisch sehr aufwendig, wurde aber auf Fachveranstaltungen bereits demonstriert. Der **Hybrid-Join-Status** eines Geräts lässt sich hingegen derzeit nicht manipulieren und stellt somit eine zuverlässige Absicherungsmethode dar.

Wenn du Richtlinien wie diese korrekt konfigurierst und testweise implementierst, kannst du mit Conditional Access eine robuste Zugriffskontrolle aufbauen. Wichtig ist dabei, nicht zu viele Sonderregeln zu etablieren und stets mit Bedacht vorzugehen. Im nächsten Abschnitt kannst du dann die Integration bestehender MFA-Regeln analysieren und bei Bedarf optimieren.

Im Kontext der Geräteplattform-Einschränkungen wurde diskutiert, wie du über Intune differenzierte Richtlinien anwenden kannst, um die Verwaltung und Kontrolle von Geräten benutzerbasiert zu gestalten. In manchen Umgebungen werden verschiedene Gruppenrichtlinien definier, die über **Elder** mit dem **MDM-System** synchronisiert werden. Dies erlaubt, Richtlinien spezifisch auf Benutzer zu beziehen, was unter anderem **Gerätewechsel** künftig einfacher und strukturierter gestaltet.

Wesentlich ist dabei, dass du innerhalb der Richtlinie festlegen kannst, ob beispielsweise „**MMD personally owned**“ Geräte erlaubt sein sollen oder nicht. Diese Einstellung kann individuell gesetzt und anschließend über „**Next**“ weiter konfiguriert werden. Besonders wichtig: Du hast hier die Möglichkeit, diese Einschränkungen gezielt auf bestimmte **Benutzergruppen** anzuwenden. Im Gegensatz zur **globalen Konfiguration**, die für alle Benutzer gleichermaßen gilt, erlaubt dir dieser Weg eine differenzierte und gruppenbasierte Steuerung.

Diese Funktion findest du unter **Device Enrollment Restrictions → Groups**, wo du benutzerdefinierte Einschränkungen definieren und zielgerichtet zuweisen kannst.

Kapitel 23: Config Refresh – Konfigurationssicherheit und Performancestabilisierung

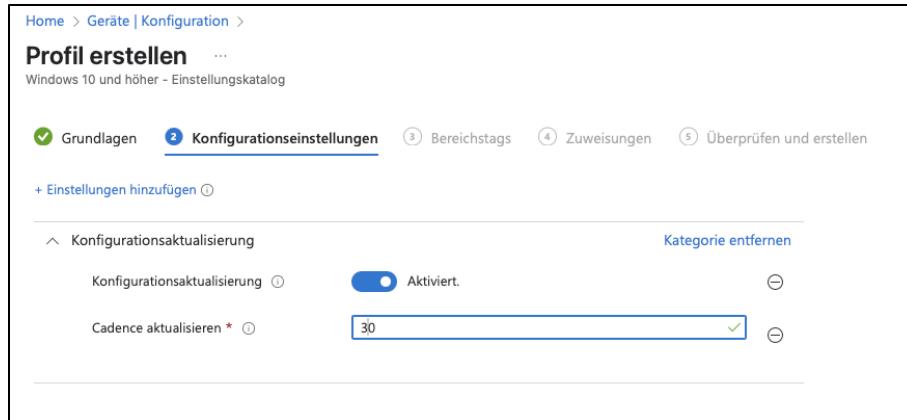
Ein weiterer Bestandteil moderner Gerätekonfiguration in Microsoft Intune ist die Funktion **Config Refresh**. Sie dient dazu, die Konsistenz und Integrität der Konfiguration auf verwalteten Endgeräten aktiv sicherzustellen – sowohl unter Sicherheitsaspekten als auch im Hinblick auf Stabilität und Performance. Du solltest diese Funktion unbedingt in deine Verwaltungsstrategie integrieren.

Das zugrunde liegende Prinzip von Config Refresh besteht darin, dass Geräte in regelmäßigen Intervallen automatisch ihre Richtlinien erneut abfragen und anwenden. Das bedeutet konkret: Sollte es zu einem externen Vorfall kommen – beispielsweise durch Malware, einen externen Eingriff oder einen anderen sicherheitsrelevanten Breach – bei dem Konfigurationseinstellungen auf dem Client manipuliert wurden, dann wird dieser Zustand durch die automatische Aktualisierung der Konfiguration wieder zurückgesetzt. Damit lässt sich die Angriffsfläche bei kompromittierten Geräten wirksam reduzieren.

Ein zweiter Vorteil dieser Funktion liegt in der **Performanceoptimierung**. Durch den regelmäßigen Refresh der Konfigurationen wird sichergestellt, dass Richtlinien und Einstellungen ohne Verzögerung greifen. Gerade bei Clients, die längere Zeit nicht mit dem Netzwerk verbunden waren oder bei denen sich durch Benutzerinteraktionen Konfigurationselemente verändert haben, hilft Config Refresh dabei, den gewünschten Zustand schnell wiederherzustellen.

Die technische Umsetzung ist einfach. In der Intune-Konsole kannst du das Feature im Rahmen der Gerätekonfiguration aktivieren. Sobald Config Refresh eingerichtet ist, läuft der Abgleich der Richtlinien zyklisch im Hintergrund. Du musst also keine manuelle Interaktion durchführen – die Richtliniensynchronisierung geschieht automatisch und fortlaufend.

Ein zusätzlicher Effekt besteht darin, dass sich Geräte, die aus dem Unternehmenskontext herausgelöst wurden (z. B. durch nicht genehmigte Maßnahmen am Client), schneller wieder in einen verwalteten Zustand überführen lassen. Die regelmäßige Anwendung der Konfigurationsrichtlinien stellt somit nicht nur ein Sicherheitsinstrument dar, sondern kann auch als Mechanismus zur Wiederherstellung des Compliance-Zustands genutzt werden.



Home > Geräte | Konfiguration >

Profil erstellen ...

Windows 10 und höher - Einstellungskatalog

Grundlagen Konfigurationseinstellungen Bereichstags Zuweisungen Überprüfen und erstellen

+ Einstellungen hinzufügen

Konfigurationsaktualisierung Aktiviert.

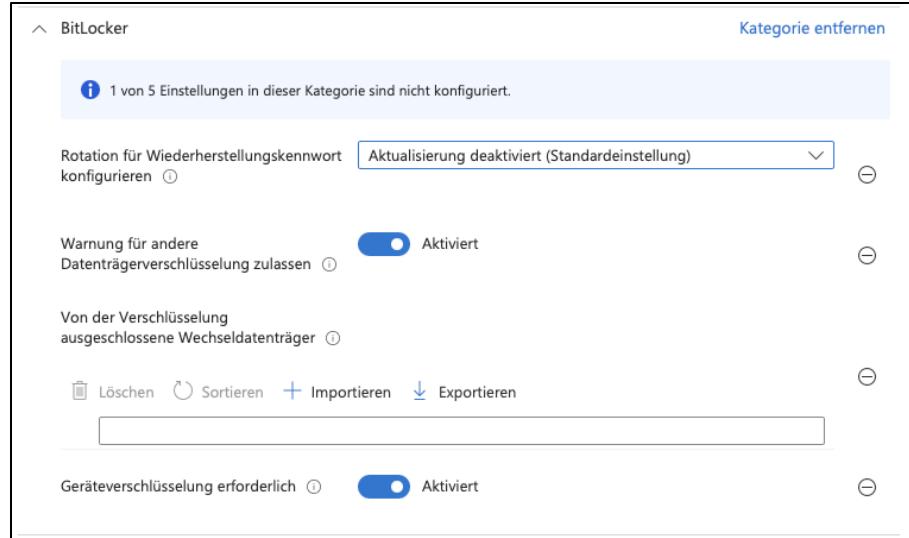
Cadence aktualisieren * 30

Bild 118: Config refresh

Kapitel 24: BitLocker-Verschlüsselung und Konfigurationsunterschiede in Intune

Ein wichtiger Aspekt beim Schutz von Endgeräten ist die **BitLocker Verschlüsselung**. Diese Maßnahme gilt mittlerweile in vielen Unternehmen als Standard, insbesondere im Kontext von Microsoft Intune.

Zunächst kannst du im Intune-Portal unter den **Konformitätsrichtlinien** die BitLocker-Verschlüsselung aktivieren. Wenn du dort den Punkt „Require BitLocker“ aktivierst, siehst du jedoch, dass der Funktionsumfang in diesem Bereich recht begrenzt ist. In der Regel steht dort nur die Option „Require device encryption“ zur Verfügung. Das heißt, du kannst grundsätzlich verlangen, dass das Gerät verschlüsselt sein muss, jedoch ohne detaillierte Konfigurationsmöglichkeiten. Für viele Einsatzszenarien reicht das nicht aus.



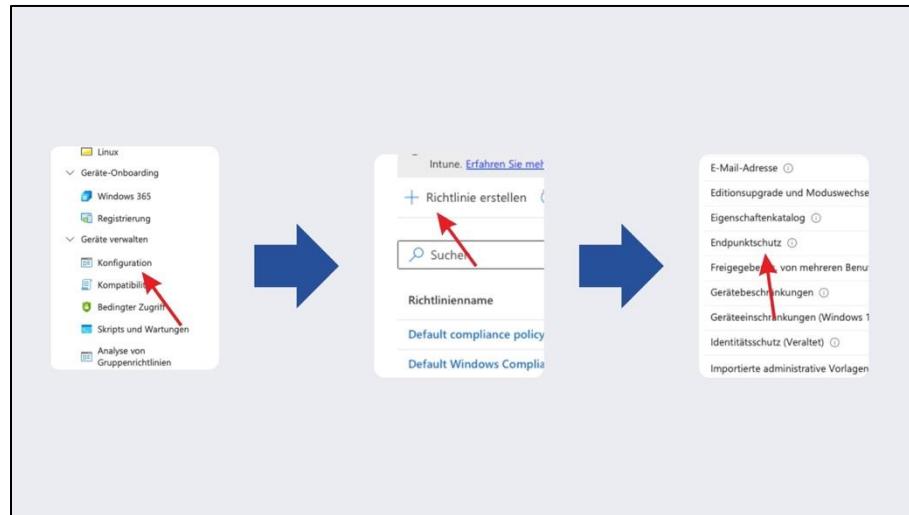
The screenshot shows the BitLocker configuration page. At the top, there's a header with the category name "BitLocker" and a "Kategorie entfernen" (Remove category) button. Below the header, a message says "1 von 5 Einstellungen in dieser Kategorie sind nicht konfiguriert." (1 of 5 settings in this category are not configured). There are three main configuration items listed:

- "Rotation für Wiederherstellungskennwort konfigurieren" (Configure recovery key rotation) - Status: Aktualisierung deaktiviert (Standardeinstellung) (Update disabled (standard setting)).
- "Warnung für andere Datenträgerverschlüsselung zulassen" (Allow other drives to be encrypted) - Status: Aktiviert (Enabled).
- "Von der Verschlüsselung ausgeschlossene Wechseldatenträger" (Excluded removable drives from encryption) - Status: Aktiviert (Enabled).

At the bottom of the list, there are buttons for "Löschen" (Delete), "Sortieren" (Sort), "Importieren" (Import), and "Exportieren" (Export). Below these buttons, another section titled "Geräteverschlüsselung erforderlich" (Encryption required) has its status set to "Aktiviert" (Enabled).

Bild 119: BitLocker-Verschlüsselung

Um mehr Steuerungsmöglichkeiten zu erhalten, musst du stattdessen in den Bereich **Gerätekonfiguration** wechseln. Du findest dort unter *Devices → Configuration* die Option, ein neues Profil zu erstellen. Wähle dazu den Pfad *Templates → Endpoint protection*, um ein neues Profil zur Konfiguration der Geräteeinstellungen zu erstellen. Wähle dort „Windows Encryption“, um die Verschlüsselungseinstellungen gezielt zu steuern.



The diagram illustrates the navigation steps to create a new Endpoint Protection policy:

- The first panel shows the "Devices" navigation menu with "Konfiguration" selected. A red arrow points to the "Kompatibilität" (Compatibility) option under "Konfiguration".
- The second panel shows the "Richtlinie erstellen" (Create policy) screen. A red arrow points to the "+" button to start creating a new policy.
- The third panel shows the "Richtlinienname" (Policy name) input field and the "Default compliance policy" and "Default Windows Complia" dropdowns. A red arrow points to the "Freigegeben" (Shared) link in the right-hand sidebar, which lists various policy-related options like "E-Mail-Adresse", "Editionsupgrade und Moduswechsel", and "Endpunktsschutz".

Bild 120: Endpoint protection

In diesem erweiterten Konfigurationsbereich kannst du wesentlich detaillierter festlegen, wie BitLocker auf den Geräten eingesetzt werden soll. Du hast die Möglichkeit, die **Verschlüsselungsmethode** festzulegen, z. B. ob XTS-AES mit 128 oder 256 Bit verwendet werden soll. Zusätzlich kannst du entscheiden, ob Benutzer gewarnt werden sollen, wenn eine inkompatible Verschlüsselung entdeckt wird. Ebenfalls konfigurierbar sind Anforderungen an das Vorhandensein eines **TPM (Trusted Platform Module)** sowie der Einsatz einer **PIN-Eingabe beim Systemstart**, inklusive der Frage, ob diese Eingabe verpflichtend oder optional sein soll.

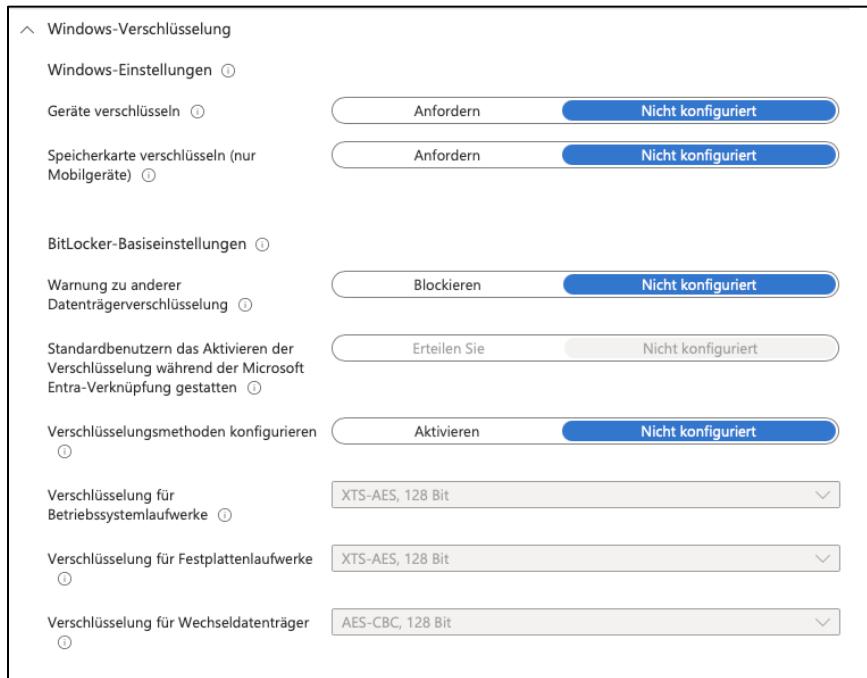


Bild 121: Windows Encryption

Diese erweiterten Steuerungsoptionen stehen dir nur im Gerätekonfigurationsprofil zur Verfügung – nicht aber in der einfachen Konformitätsrichtlinie. Das bedeutet für dich in der Praxis: Möchtest du BitLocker vollständig und kontrolliert in deiner Umgebung ausrollen, solltest du die Konfiguration **nicht nur über die Konformitätsrichtlinien, sondern ergänzend über ein dediziertes Konfigurationsprofil** im Settings Catalog oder unter Templates vornehmen.

Dabei ist zu beachten, dass Microsoft inzwischen neue Einstellungen bevorzugt im **Settings Catalog** bereitstellt, während ältere Vorlagen wie die Templates zum Teil noch zusätzliche, nicht migrierte Funktionen enthalten. In der Übergangsphase ist es daher notwendig, beide Pfade im Blick zu behalten. Viele Einstellungen sind bislang nicht vollständig in den neuen Settings Ca-

talog übernommen worden. Das führt dazu, dass einige Optionen im alten Template-Modell verfügbar sind, aber nicht im neuen Settings Catalog. Dieser Umstand kann je nach Anwendungsfall zur Entscheidung führen, weiterhin auf Templates zurückzugreifen – zumindest solange, bis Microsoft die vollständige Funktionalität im Settings Catalog abbildet.

Kapitel 25: OneDrive und der Known Folder Move (KFM)

Ein weiterer zentraler Bestandteil der modernen Client-Verwaltung ist der Einsatz von OneDrive, insbesondere in Verbindung mit dem sogenannten **OneDrive Known Folder Move (KFM)**. Diese Funktion spielt eine wichtige Rolle beim Schutz und der Sicherung von Benutzerdaten und sollte in einem modernen Arbeitsplatzkonzept nicht fehlen.

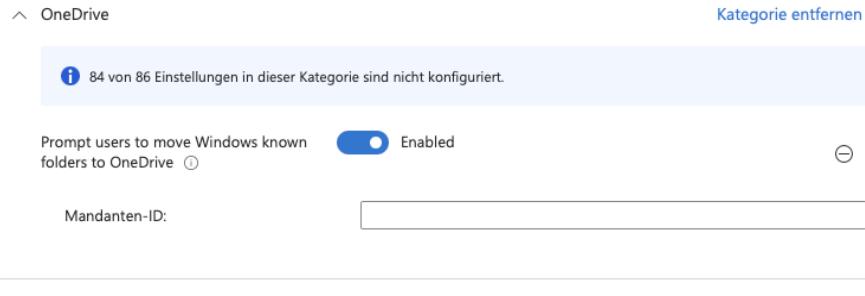
Mit dem Known Folder Move kannst du festlegen, dass die bekannten Windows-Ordner **Desktop**, **Dokumente** und **Bilder** automatisch mit OneDrive synchronisiert werden. Ziel ist es, dass Benutzer ihre Daten nicht manuell in einen OneDrive-Ordner verschieben müssen, sondern dass bestehende Inhalte an ihrem gewohnten Speicherort verbleiben, jedoch im Hintergrund automatisch in die Cloud repliziert werden.

Die Umsetzung erfolgt dabei über eine Richtlinie, die zentral per Intune verteilt werden kann. Konkret nutzt du dafür den Punkt "**Prompt users to move Windows known folders to OneDrive**" in dem Einstellungskatalog für OneDrive.

> Prompt users to move Windows known folders to OneDrive

Bild 122: Prompt

Diese Einstellung sorgt dafür, dass dem Benutzer beim Anmelden ein Hinweis angezeigt wird, mit dem er bestätigen kann, dass seine Daten aus den bekannten Ordnern in OneDrive übertragen werden sollen. Zusätzlich muss hier die **Tenant ID** angegeben werden, damit die Verbindung zum richtigen Mandanten erfolgt.



The screenshot shows a configuration page for OneDrive in Microsoft Intune. At the top, there's a navigation bar with 'OneDrive' and a 'Kategorie entfernen' (Delete category) button. Below this, a message box indicates '84 von 86 Einstellungen in dieser Kategorie sind nicht konfiguriert.' (84 of 86 settings in this category are not configured). The main section contains a setting titled 'Prompt users to move Windows known folders to OneDrive' with a status of 'Enabled'. There's also a 'Mandanten-ID:' field with a placeholder box. A small note at the bottom says 'Bild 123: Tenant-ID'.

Sobald der Benutzer dieser Aufforderung zustimmt, werden alle Daten aus den bekannten Ordnern in das entsprechende Verzeichnis im OneDrive verschoben. Von diesem Moment an erfolgt die Synchronisation automatisch. Das bedeutet auch: Sollte es zum Ausfall eines Geräts kommen – beispielsweise durch einen Defekt der SSD – bleiben die Daten erhalten, da sie nicht lokal, sondern in der Cloud gesichert wurden.

Ein weiterer Vorteil ergibt sich beim Gerätewechsel. Meldet sich ein Benutzer an einem neuen Windows-Client an, werden die Inhalte der bekannten Ordner automatisch wiederhergestellt. Dies vereinfacht die Migration erheblich und reduziert den Aufwand für manuelle Datensicherung und -übertragung.

Kapitel 26: Konfiguration der LAPS-Funktion in Microsoft Intune

Um mit der Konfiguration zu beginnen, navigierst du innerhalb von Intune zum Bereich **Endpoint Security** und wählst dort den Abschnitt **Account Protection** aus. Unter diesem Menü findest du die Option **Local Administrator Password Solution (Windows LAPS)**. Sobald du diese Richtlinie ausgewählt hast, findest du im unteren Bereich die Konfigurationseinstellungen (**Configuration settings**), die du über die Schaltfläche **Edit** anpassen kannst.



Bild 124: Laps Configuration Settings

Ein wesentlicher Punkt in der Konfiguration ist die Festlegung, wohin das generierte Passwort gespeichert werden soll. Du kannst zwischen **Azure AD** und **Active Directory** wählen. Dies richtet sich maßgeblich danach, ob deine Geräte cloudbasiert oder hybrid verwaltet werden. In reinen Cloud-Umgebungen ist die Speicherung in Azure AD sinnvoll und notwendig, da dort das Attribut zum Speichern des Passworts zur Verfügung steht.

Ein weiterer Konfigurationspunkt ist das **Passwortalter (Password Age)**. Hier definierst du, nach wie vielen Tagen das lokale Administratorpasswort automatisch erneuert werden soll. Dieser Wert sollte praxisgerecht gewählt werden – nicht zu kurz, um unnötige Rotation zu vermeiden, aber auch nicht zu lang, um Sicherheitsrisiken durch veraltete Passwörter zu minimieren.

Zusätzlich kannst du einen **benutzerdefinierten Namen** für den lokalen Administrator-Account angeben. Alternativ kann auch der Standardname verwendet werden. Die Wahl des Accountnamens hängt von deinen internen Sicherheitsvorgaben ab. Häufig entscheiden sich Unternehmen dafür, einen eigenen eindeutigen Namen zu verwenden, um den bekannten Standard-Account (Administrator) zu vermeiden. Dieser Standardaccount ist oft ein Ziel bei Brute-Force-Angriffen oder im Fall von Sicherheitsvorfällen. Ein abweichender Name bietet hier eine zusätzliche Schutzschicht, indem er das Angriffsziel weniger offensichtlich macht.

Ein weiterer Sicherheitsaspekt betrifft die Einstellungen zur **Passwortkomplexität (Password Complexity)** und **Passwortlänge (Password Length)**. In der LAPS-Richtlinie kannst du festlegen, ob das Passwort beispielsweise Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen

enthalten muss und wie viele Zeichen es mindestens umfassen soll. Diese Vorgaben sollten in Übereinstimmung mit deinen unternehmensweiten Passwort-Richtlinien gewählt werden.

Diese LAPS-Konfiguration stellt sicher, dass jedes verwaltete Gerät über ein sicheres, individuelles und regelmäßig erneuertes lokales Administratorkennwort verfügt. Dies ist insbesondere in Situationen wichtig, in denen Geräte vorübergehend aus der Verwaltung fallen, bei Vor-Ort-Reparaturen oder in Netzwerkszenarien mit eingeschränkter Konnektivität.

Nach der allgemeinen Konfiguration von LAPS (Local Administrator Password Solution) ist es wichtig, sich mit den erweiterten Optionen zur Passwort- und Kontenverwaltung auseinanderzusetzen. Standardmäßig ist bei der Passwortgenerierung das Profil **Default** aktiv. Alternativ stehen jedoch weitere Konfigurationsmöglichkeiten zur Verfügung, etwa die Variante **Special Characters Improved Readability**. Diese Einstellung wurde testweise eingesetzt, jedoch als weniger benutzerfreundlich bewertet. Daher hat man sich in vielen Fällen auf die Kombination aus **Großbuchstaben, Kleinbuchstaben und Zahlen** verständigt.

Wichtig zu wissen: Im Kontext einer Cyber-Versicherung gelten oft strengere Anforderungen. So wird häufig verlangt, dass Passwörter **Sonderzeichen enthalten** und **mindestens 16 Zeichen** lang sind. Diese Vorgaben sollten bei entsprechender vertraglicher Bindung zwingend eingehalten werden.

Ein weiterer Aspekt betrifft das Verhalten des Systems nach der Anmeldung mit dem LAPS-Konto. In der Konfiguration besteht die Möglichkeit, bestimmte Aktionen nach der Nutzung zu definieren. Üblich ist beispielsweise die Option „**Reset**“ – das bedeutet, dass das Passwort nach Verwendung automatisch zurückgesetzt wird. Alternativ kann auch eine Kombination aus **Passwort-Reset und Abmeldung des Accounts (Logout)** oder ein **Reboot des Geräts** gewählt werden. In der Praxis wird häufig die Variante genutzt, bei der das Passwort zurückgesetzt und gleichzeitig der Benutzer ausgeloggt wird.

Zusätzlich kann definiert werden, **nach wie vielen Stunden** die Rücksetzung erfolgen soll. Diese Konfiguration sorgt dafür, dass der lokale Administratorzugriff immer nur kurzfristig gültig ist, was die Sicherheit deutlich erhöht.

Eine neue Funktion innerhalb von LAPS ist die Möglichkeit, nicht nur das Passwort zufällig generieren zu lassen, sondern auch den **Benutzernamen für den lokalen Administratoraccount**. Diese Option wurde erst kürzlich ergänzt und erweitert die Möglichkeiten zur Absicherung durch zusätzliche Variabilität im System.

Die **Einsicht des aktuellen lokalen Administratorpassworts** erfolgt direkt über den Client im Intune-Portal. Dazu navigierst du zum entsprechenden Gerät und findest unter der Rubrik **Local Admin Password** die Option „**Show local administrator password**“. Nach Auswahl dieser Funktion wird das aktuelle Kennwort angezeigt. Dieses wird automatisch entweder **nach einmaliger Verwendung** oder **nach Ablauf einer definierten Anzahl von Tagen** (z. B. sieben oder vierzehn Tagen) durch ein neues ersetzt. Die genaue Dauer lässt sich innerhalb der LAPS-Richtlinie individuell festlegen.

Diese Mechanismen tragen entscheidend dazu bei, den Zugriff auf lokale Administratorkonten kontrolliert, nachvollziehbar und vor allem sicher zu gestalten.

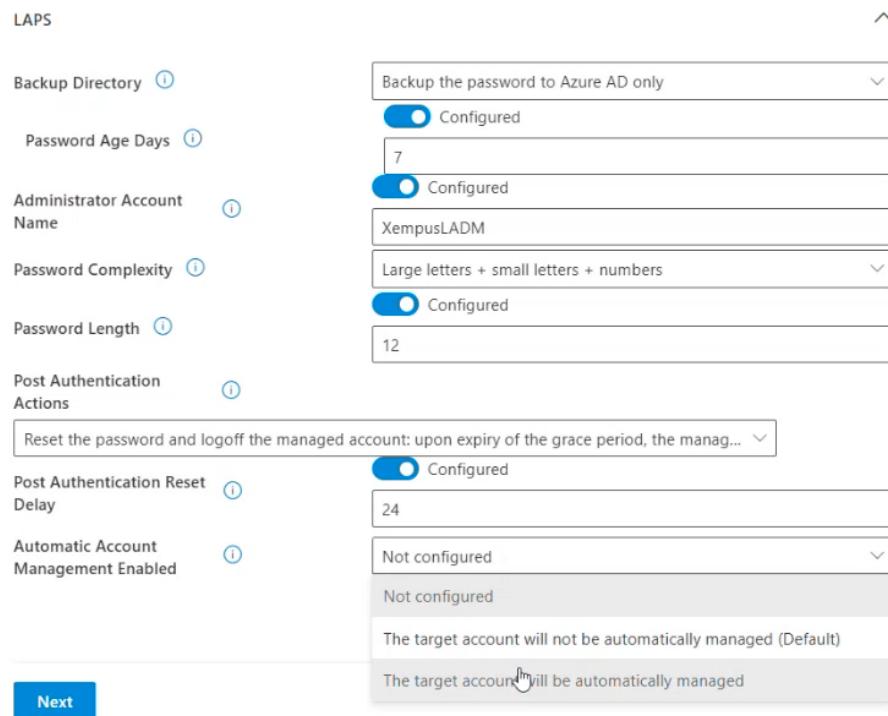


Bild 125: LAPS Einstellungen

Kapitel 27: Geräteeinschränkungen und ADMX-Import in Intune

In der Verwaltung deiner Windows-Geräte über Microsoft Intune empfiehlt es sich, regelmäßig die Konfigurationsprofile zu überprüfen und gezielt Richtlinien zu definieren, die sicherheits- und unternehmensrelevante Funktionen betreffen. Ein bewährter Ansatz ist es, mit einem konsistenten Set an Einstellungen zu arbeiten, die in vielen Umgebungen als Basiskonfiguration sinnvoll sind.

Ein typisches Beispiel ist der Bereich „**Device Restrictions**“, speziell die „**Experience**“-Einstellungen. Hier findest du Optionen wie die Deaktivierung von **Cortana**, die Sperrung der **manuellen MDM-Registrierung** sowie das Management von **Spotlight-Features**. Auch wenn Dienste wie Cortana in der Praxis oft kaum noch relevant erscheinen, solltest du diese bewusst blockieren, da sie systemseitig weiterhin aktivierbar sind. Eine zentrale Steuerung dieser Punkte trägt zur Homogenisierung der Benutzererfahrung und zur Reduzierung potenzieller Angriffsflächen bei.

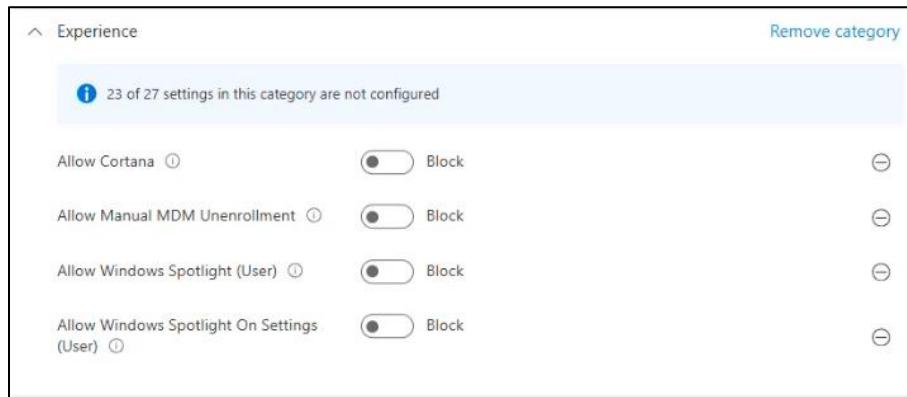


Bild 126: Experience

Ebenso bietet dir Intune die Möglichkeit, Richtlinien für die **Kontrolle von Apps** festzulegen. Du kannst etwa den **Microsoft Store** vollständig blockieren, wenn du vermeiden möchtest, dass Benutzer eigenständig Applikationen installieren. Im Unternehmenskontext ist die Intune-verwaltete **Unternehmensportal-App** der bevorzugte Weg, um Software bereitzustellen. Die Unternehmensportal-App übernimmt dabei die Funktion eines firmeninternen App-Stores und

bietet durch automatisierte Updates und zentrale Verwaltung eine zuverlässige Grundlage für die Softwareverteilung.

Ein weiterer zu beachtender Bereich ist die Einstellung zum **Gerätesperrverhalten**. Über die Richtlinie „Device Lock“ kannst du beispielsweise festlegen, nach wie vielen Minuten der Inaktivität ein Gerät automatisch gesperrt wird – ein klassischer Bestandteil aus der GPO-Welt, der in Intune ebenfalls abgebildet werden kann.

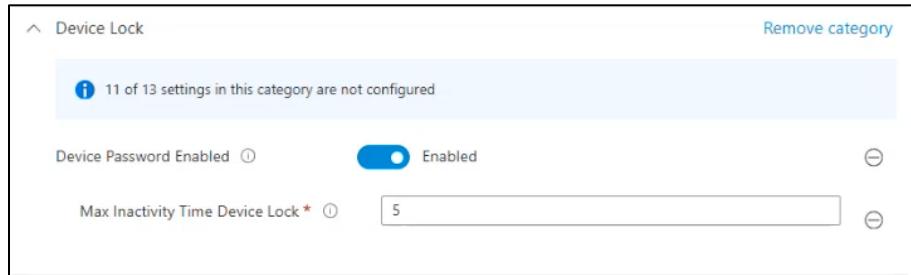


Bild 127: Device Lock

Falls du bereits eine etablierte GPO-Struktur in deiner lokalen Umgebung pflegst und nicht jede Richtlinie manuell nachbauen möchtest, stellt Intune eine **Importfunktion für ADMX-Dateien** zur Verfügung. Diese findest du unter dem Punkt „**Import ADMX**“ im Konfigurationsbereich. Hier kannst du sowohl die **.admx-Datei** (für die Richtliniendefinitionen) als auch die zugehörige **.adml-Datei** (für Sprachressourcen) hochladen.

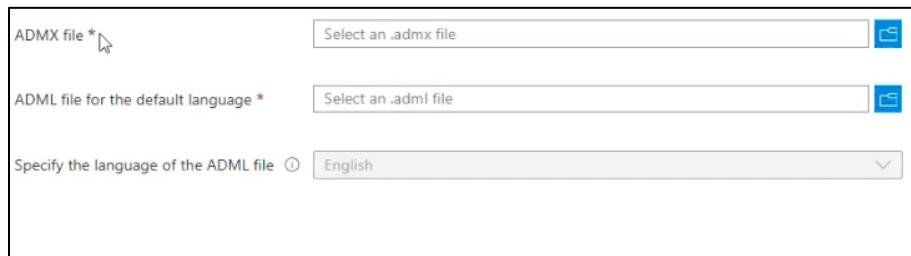


Bild 128: ADMX File & ADML File

Nach erfolgreichem Upload erscheinen die Richtlinien im **Settings Catalog** von Intune und lassen sich dort wie gewohnt auswählen und anwenden. Der Vorteil: Die Konfiguration wird exakt übernommen, wie sie ursprünglich lokal definiert war. So kannst du bestehende

Gruppenrichtlinien effizient in die cloudbasierte Verwaltung überführen, ohne sie komplett neu erstellen zu müssen. Das spart Zeit und erhöht die Konsistenz in der Policy-Verwaltung über unterschiedliche Plattformen hinweg.

Kapitel 28: Erweiterte Geräteinventarisierung mit dem Properties-Katalog in Intune

In den Gerätekonfigurationsrichtlinien unter Intune solltest du den sogenannten **Properties-Katalog** berücksichtigen. Dieser Katalog bietet dir die Möglichkeit, die **erweiterte Inventarisierung** von Windows-Geräten zu aktivieren.

Das Thema Inventarisierung und Reporting wird im Kontext von Intune allgemein als eher schwach bewertet. Viele empfinden die verfügbaren Funktionen als mittelmäßig. Umso wichtiger ist es, dass du die vorhandenen Optionen bestmöglich nutzt. Der Properties-Katalog funktioniert dabei vom Aufbau her ähnlich wie der bekannte Settings-Katalog. Du kannst gezielt auswählen, welche Hardware-Informationen Intune bei der Inventarisierung eines Geräts erfassen soll.

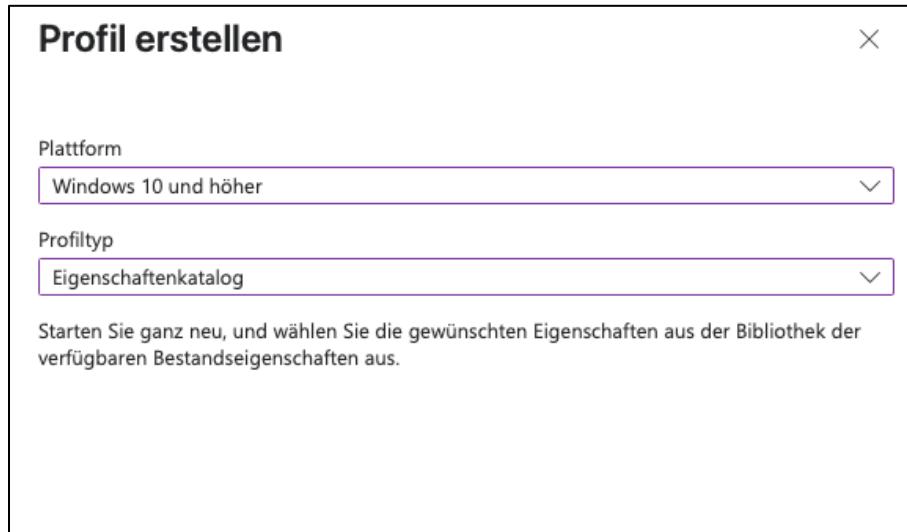


Bild 129: Properties-Katalog

Zu den auswählbaren Daten gehören unter anderem Informationen wie **CPU-Typ**, **CPU-Status**, **Prozessormodell**, **Hersteller**, **Festplattenbeschreibung**, **Festplattenname** und **Größe in Byte**. All diese Informationen können durch die Konfiguration im Properties-Katalog gesammelt und anschließend im Intune-Portal angezeigt werden.

Wenn du im Intune-Portal auf **Devices > Windows** gehst und dort ein Gerät auswählst, findest du unter anderem den sogenannten **Resource Explorer**. Dieser zeigt dir genau die Informationen an, die du zuvor über den **PropertiesPicker** definiert hast. Wenn du den Properties-Katalog nicht nutzt, sind die angezeigten Informationen unter dem Menüpunkt **Hardware** deutlich eingeschränkter. Du siehst dort dann lediglich grundlegende Daten wie **Betriebssystemversion**, **Sprache**, **Speichermodell** und **Seriennummer**.

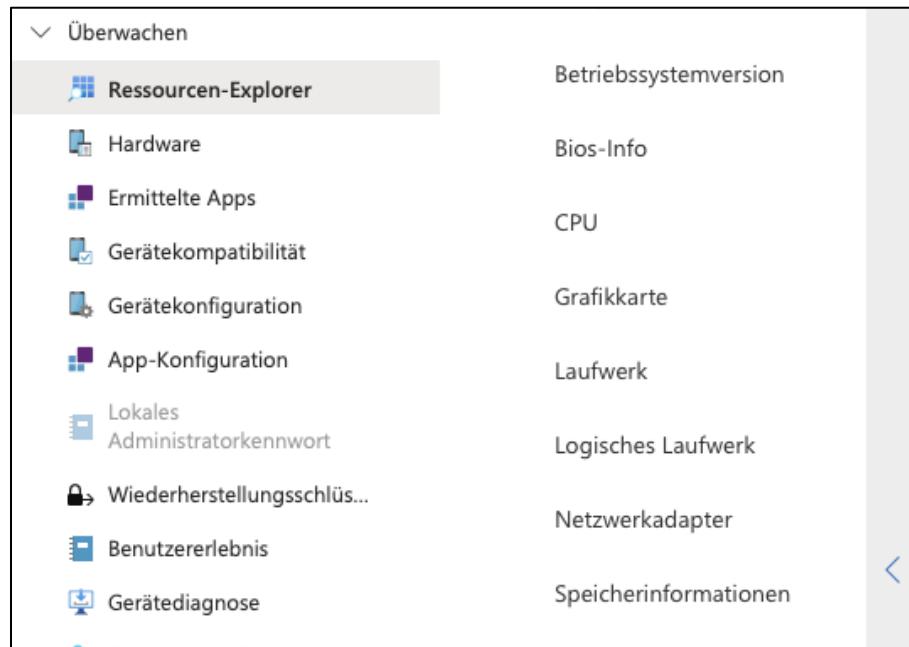


Bild 130: Ressourcen-Explorer

Der Einsatz des Properties-Katalogs ermöglicht dir also eine deutlich detailliertere Geräteinventarisierung, als es mit den Standardoptionen ohne zusätzliche Konfiguration möglich wäre.

Kapitel 28: Managed Apps, Discovery Apps und Geräte-Diagnose in Intune

In Microsoft Intune unterscheidest du bei der Verwaltung von Anwendungen grundsätzlich zwischen zwei Kategorien: **Discovery Apps** und **Managed Apps**. Diese Differenzierung ist entscheidend, wenn du beispielsweise im Rahmen von Supportfällen oder beim Troubleshooting nach Ursachen suchst.

Discovery Apps bezeichnen dabei Anwendungen, die bereits auf einem Gerät vorhanden waren – unabhängig davon, ob sie durch den Benutzer selbst installiert oder durch andere Installationswege auf das System gelangt sind. Diese Apps sind demnach aus Sicht von Intune „entdeckt“, wurden jedoch nicht über Intune bereitgestellt.

Managed Apps hingegen sind die Anwendungen, die du explizit über Intune verteilt und verwaltet hast. Sie wurden entweder über den Microsoft Store, per Win32-Paketierung oder andere unterstützte Mechanismen bereitgestellt und sind direkt an die Intune-Verwaltung gekoppelt.

Wenn du bei bestimmten Geräten oder Installationen auf Probleme stößt, hast du mehrere Wege, um die Ursachen einzuschränken. Zunächst kannst du in der Geräteübersicht in Intune über die **Device Configuration** prüfen, welche Richtlinien ein Gerät erhalten hat.

Hardware	Richtlinie	Angemeldeter Benutzer
Erermittelte Apps	Default EDR policy for all devices	aaron@siller.consulting
Gerätekompatibilität	Default EDR policy for all devices	Systemkonto
Gerätekonfiguration	Enroll_Defender	aaron@siller.consulting
App-Konfiguration	Enroll_Defender	Systemkonto
Lokales Administratorkennwort	Firewall Windows default policy	Systemkonto
Wiederherstellungsschlüssel	Firewall Windows default policy	aaron@siller.consulting
Benutzererlebnis	Intune data collection policy	Systemkonto
Gerätediagnose	Intune data collection policy	aaron@siller.consulting
Gruppenmitgliedschaft	LAPS	aaron@siller.consulting

Bild 131: Gerätekonfiguration

Wenn du in eine bestimmte Richtlinie hinein navigierst, findest du dort die einzelnen **Einstellungsnamen (Setting Names)** sowie deren **Status**. Diese Einstellungen können entweder auf einem eigenen URI-Schema (z. B. ./Device/Vendor/MSFT/...) basieren oder aus integrierten Vorlagen stammen. Bei fehlerhaften Richtlinien wird dir ein **Fehlercode** angezeigt. Die Fehlerdiagnose erfolgt dabei in der Praxis häufig durch manuelle Recherche des Fehlercodes – z. B. über Suchmaschinen, da Intune selbst meist keine Erklärung dazu liefert.

Name	Status	Fehlercode
Accounts Enable Administrator Account Status	 Erfolgreich	
Accounts Rename Administrator Account	 Erfolgreich	

Bild 132: Richtlinie

Ein ähnlicher Ablauf gilt auch für deine **bereitgestellten Anwendungen** (Managed Apps). Wenn du feststellst, dass z. B. eine bestimmte Applikation nicht ordnungsgemäß installiert wurde, kannst du innerhalb der App-Übersicht auf die Detailansicht eines Geräts wechseln. Dort siehst du die **Installationsschritte** sowie potenzielle **Fehlermeldungen und Codes**. Diese geben dir Anhaltspunkte, ob z. B. die Installationsdateien, Abhängigkeiten oder Benutzerberechtigungen ursächlich für den Fehler sind.

Für eine tiefergehende Analyse stellt dir Intune zudem die Funktion **Collect Diagnostics** zur Verfügung. Diese erreichst du in der Geräteübersicht eines Endgeräts über den Punkt **Overview → Collect Diagnostics**. Wenn du diese Funktion aktivierst, wird eine ZIP-Datei generiert, die sämtliche relevanten Ereignisprotokolle aus der **Windows-Ereignisanzeige (Event Viewer)** beinhaltet. Diese Datei kannst du zur weiteren Analyse lokal speichern oder über zentrale Ticketsysteme weitergeben.

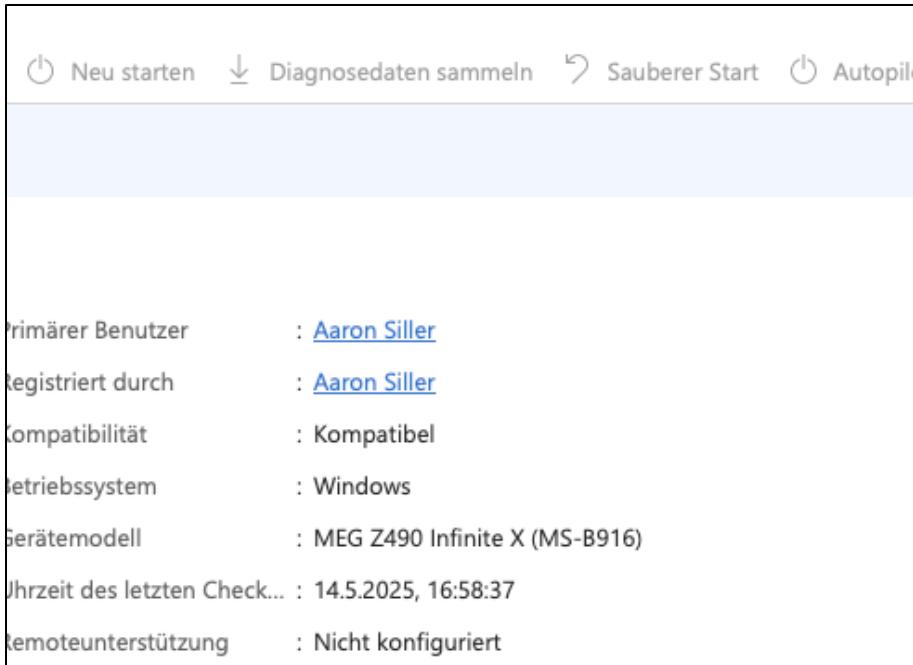


Bild 133: Diagnosedaten sammeln

Neben der serverseitigen Analyse über das Intune-Portal kannst du auch direkt auf dem Client arbeiten. Im Unternehmensportal auf dem jeweiligen Gerät hast du die Möglichkeit, manuell eine **Synchronisierung** anzustoßen. Alternativ kannst du im Intune-Portal unter dem jeweiligen Gerät die **Sync-Funktion** nutzen, um eine erneute Richtlinien- und App-Abfrage zu erzwingen.

Trotz dieser Möglichkeiten solltest du dir bewusst sein, dass sich dadurch die generelle Geschwindigkeit von Intune nicht erhöhen lässt. Insbesondere bei komplexen oder mehrfach verschachtelten Richtlinien können Synchronisation und Fehlerbehebung mitunter Zeit beanspruchen. Die genannten Werkzeuge unterstützen dich jedoch dabei, systematisch vorzugehen und fundierte Entscheidungen auf Basis belastbarer Daten zu treffen.

Im Rahmen der erweiterten Geräteinventarisierung in Microsoft Intune wurde die Frage gestellt, unter welchen Voraussetzungen **Discovered Apps** auf einem Gerät angezeigt werden. Der Hintergrund dabei war, dass bei einigen Geräten, die exemplarisch in Intune eingebunden wurden, keine Anwendungen unter diesem Punkt aufgeführt waren.

Ein entscheidender Faktor dabei ist die Art und Weise, wie ein Gerät in die Microsoft Entra ID (ehemals Azure AD) eingebunden wurde. In einem konkreten Beispiel wurde festgestellt, dass das betreffende Gerät den Status „**Microsoft Entra registered**“ trug. Dieser Registrierungstyp ist eingeschränkt und ermöglicht nur eine begrenzte Inventarisierung. Das bedeutet, du bekommst keine vollständigen Informationen über die installierte Software oder die komplette Hardwareausstattung des Clients.

Die Ursache für diesen Status ist häufig, dass sich ein Benutzer mit seinem Unternehmens- oder Schulkonto direkt am Gerät anmeldet, ohne dass das Gerät vorher vollständig über Intune oder den Autopilot-Prozess registriert wurde. Eine solche Anmeldung führt zur Registrierung in der Entra ID, aber nicht zur vollständigen Verwaltung über Intune.

Um dieses Problem zu beheben und eine vollständige Geräteverwaltung inklusive detaillierter Inventarisierung zu ermöglichen, gibt es mehrere Optionen:

1. Gerät entfernen und neu verbinden:

Du kannst das bestehende Gerät zunächst aus der Entra ID und ggf. aus Intune entfernen. Das erfolgt über die Einstellungen am Gerät:

- Navigiere zu den Kontoeinstellungen → Zugriff auf Arbeits- oder Schulkonto
- Trenne die Verbindung zur aktuellen Entra ID
- Anschließend kannst du das Gerät erneut verbinden. Wichtig dabei ist, nicht die E-Mail-Adresse unter dem Menüpunkt „Konto hinzufügen“ einzutragen, da dies erneut nur eine Entra-ID-Registrierung und keine vollständige Verwaltung auslöst.
Stattdessen solltest du die Option nutzen, das Gerät direkt ins MDM zu überführen oder Microsoft Entra Join auszuwählen, sofern verfügbar.

2. Verwendung des Intune Deep Links für die Registrierung:

- Alternativ kannst du einen sogenannten **Intune Deep Link** aufrufen. Dieser ermöglicht es, direkt vom Client aus die Registrierung in Intune zu initiieren.
- Wenn du diesen Link im Browser auf dem betreffenden Gerät öffnest, wirst du zur entsprechenden Registrierung geführt. Auch so erreichst du, dass das Gerät vollständig verwaltet wird.

3. Verwendung des Properties-Katalogs zur Erweiterung der Inventarisierung:

Zusätzlich kannst du, selbst wenn Geräte bereits registriert sind, die **Inventarisierung erweitern**, indem du in Intune eine neue Konfigurationsrichtlinie erstellst:

- Navigiere zu Devices → Configuration profiles → Create profile
- Wähle Windows 10 and later und als Profiltyp Settings catalog

- Suche nach dem Punkt „Properties“ oder „Erweiterte Geräteeigenschaften“ und füge dort relevante Informationen wie CPU, Disk Size, Serial Number, etc. hinzu
- Weise die Richtlinie dann den betroffenen Geräten zu.

Wichtig ist in diesem Zusammenhang zu verstehen, dass nur vollständig verwaltete Geräte (z. B. über **Microsoft Entra Join** oder **Autopilot**) die volle Funktionalität bieten, inklusive der Möglichkeit zur **vollständigen Inventarisierung** und Anzeige von **Discovered Apps**. Ein reines „Registered“-Gerät bietet lediglich eingeschränkten Zugriff auf Verwaltungsfunktionen, was gerade bei tiefergehender Kontrolle und Dokumentation zu Problemen führen kann.

Im Zusammenhang mit den Geräteplattform-Einschränkungen (Device Platform Restrictions) in Microsoft Intune wurde ein zentraler Punkt angesprochen: Wenn in deiner Umgebung viele Geräte über den Registrierungsweg „Microsoft Entra registered“ eingebunden wurden – sei es gewollt oder ungewollt – solltest du überprüfen, ob in deiner Policy für „All Users“ unter den **Eigenschaften (Properties)** bereits Einschränkungen für die Geräteplattform gesetzt wurden.

Plattformeinstellungen				
Typ	Plattform	Min	Max.	Persönliches Eigentum
Android Enterprise (Arbeitsprofil)	Erteilen Sie			Erteilen Sie
Android-Geräteadministrator	Erteilen Sie			Blockieren
iOS/iPadOS	Erteilen Sie			Erteilen Sie
macOS	Erteilen Sie	N/V	N/V	Erteilen Sie
Windows (MDM)	Erteilen Sie			Erteilen Sie

Bild 134: Platform restrictions

Wenn dort unter dem Abschnitt „**Personally owned**“ noch die Standardeinstellung „**Allow**“ gesetzt ist, besteht die Möglichkeit, dass sich Benutzergeräte ohne weitere Kontrolle über den privaten Weg bei Intune registrieren. Um dies zu verhindern, solltest du in dieser Richtlinie unter dem Punkt „**Personally owned**“ gezielt die Geräteplattformen blockieren, die in deiner Organisation nicht benötigt werden. Wenn beispielsweise macOS-Geräte nicht verwendet werden, kannst du die Plattform auf „**Block**“ setzen. Dasselbe gilt für andere Plattformen wie Android oder iOS, sofern sie im Unternehmen nicht zur Anwendung kommen.

Diese Einschränkungen beziehen sich jedoch ausschließlich auf die Verwaltung über Intune. Eine Registrierung in der **Microsoft Entra ID** kann weiterhin stattfinden – dies lässt sich über diese Plattformrichtlinie allein nicht unterbinden. Die Konsequenz daraus ist, dass Geräte zwar in der

Entra ID auftauchen, aber nicht vollständig durch Intune verwaltet werden. Das wiederum erschwert die zentrale Administration und Inventarisierung erheblich.

Ein häufiger Fehler in diesem Zusammenhang ist die nachträgliche Änderung der Geräteklassifikation über das sogenannte **Device Ownership** – also das manuelle Umstellen von „Personal“ auf „Corporate“. Auch wenn dadurch beispielsweise Informationen wie die Rufnummer im Intune-Portal angezeigt werden, hat diese Änderung **keinen Einfluss auf den eigentlichen Registrierungsweg** oder die Art der Verwaltung. Stattdessen sollte der Fokus darauf liegen, bereits beim Onboarding sicherzustellen, dass Geräte den korrekten, geplanten Registrierungsweg durchlaufen.

Zum Abschluss wurde in einem Beispiel deutlich, dass einige Geräte im Portal als „Corporate“ geführt werden, obwohl sie ursprünglich privat eingebunden waren. Hier wurde lediglich das Ownership manuell geändert – ein Vorgehen, das aus Sicht der Verwaltungsstrategie nicht empfehlenswert ist. Viel wichtiger ist es, die Plattformrestriktionen konsequent zu setzen und den richtigen Registrierungsweg von Beginn an sicherzustellen. Nur so erreichst du eine konsistente und zentral verwaltbare Geräteinfrastruktur.

Im Zusammenhang mit der Verwaltung von Apple-Geräten über Intune kam die Frage auf, warum bestimmte Gerätēupdates offenbar nur manuell durchgeführt wurden, obwohl die Zuweisung über Gruppen scheinbar korrekt konfiguriert war. In den Eigenschaften der Updatekonfiguration war klar ersichtlich, dass die entsprechenden Gerätēgruppen korrekt zugewiesen waren. Es fiel jedoch auf, dass beispielsweise das Update auf iOS 18.4 bei mehreren Geräten manuell angestoßen werden musste.

Das Verhalten ist so eigentlich nicht vorgesehen, da Intune die Updates standardmäßig pushen sollte. In einem konkreten Beispiel wurde eine Gerätēgruppe namens „MS Intune“ genutzt. Bei der Prüfung stellte sich heraus, dass diese Gruppe als Benutzergruppe angelegt war. An dieser Stelle wurde empfohlen, für solche Zwecke ausschließlich Gerätēgruppen zu verwenden – idealerweise dynamische Gerätēgruppen.

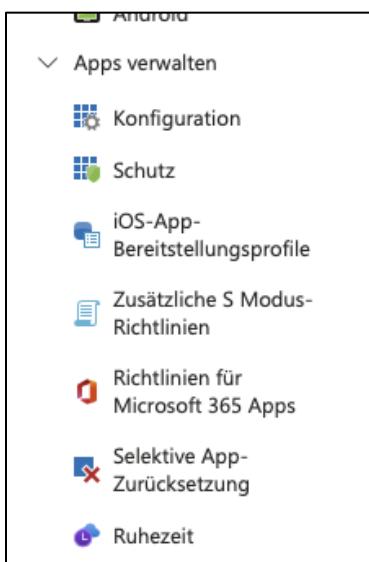
Für eine korrekte und automatische Zuweisung der Apple-Updates sollte eine dynamische Gruppe erstellt werden, die Geräte anhand ihres Betriebssystems filtert. Wenn sowohl iPhones

als auch iPads im Einsatz sind, kann eine dynamische Abfrage genutzt werden. Diese Regel stellt sicher, dass alle relevanten Geräte automatisch in die Gruppe aufgenommen werden.

Zwar lässt Intune theoretisch auch eine Zuweisung über Benutzergruppen zu, die praktische Erfahrung zeigt jedoch, dass dies bei der Verteilung von Updates zu Problemen führen kann. Um eine zuverlässige Verteilung sicherzustellen und manuelle Eingriffe zu vermeiden, ist die Verwendung von Gerätegruppen an dieser Stelle die deutlich stabilere Lösung.

Kapitel 30: App-Schutzrichtlinien, Microsoft 365 Policies und Security Baselines in Intune

Zunächst ein technischer Hinweis: Wenn ein Gerät – egal ob iOS oder Android – zum ersten Mal registriert wird, synchronisiert es sich in den ersten zwei Stunden im 15-Minuten-Takt. Danach erfolgt die Synchronisierung alle acht Stunden. Diese initial häufigere Kommunikation sorgt dafür, dass Richtlinien und Apps schnellstmöglich auf das Gerät gelangen.



Beginne nun mit dem Zugriff auf den Bereich **Apps** in Intune. Dort findest du unter anderem die Optionen **App protection**, **App configuration** und **Policies for Microsoft 365 Apps**.

Bild 135: Apps Bereich Intune

Wähle in einem ersten Schritt den Punkt „Policies for Microsoft 365 Apps“. In diesem Bereich kannst du gerätezentrale Richtlinien erstellen, die spezifisch für Anwendungen wie Word, Excel, PowerPoint, Outlook oder Access gelten.

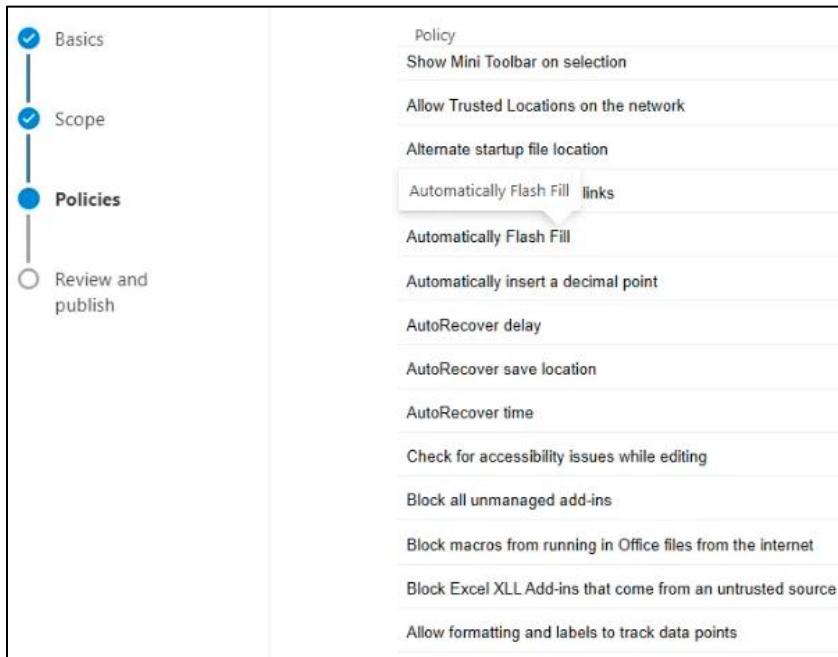
Policy configurations

[+ Create](#) [Copy](#) [↑ Reorder priority](#) [→ Export](#) [Remove](#)

Name	Priority ↑	Scope
<input type="checkbox"/> Office365-Apps-Policy1	0	User
<input type="checkbox"/> Activate Web Search Microsoft 36...	1	Tenant

Bild 136: Policy Configurations

Wenn du eine neue Richtlinie erstellst, musst du zunächst einen **Namen** und den **Scope** festlegen. Über den Scope bestimmst du, ob die Richtlinie für alle Benutzer oder nur für bestimmte Benutzergruppen gelten soll. Danach gelangst du in die **Detailkonfiguration der Office-Anwendungen**. Hier kannst du Einstellungen wie z. B. die Aktivierung von „AutoSave“ oder die Steuerung von Makros direkt definieren – ganz ohne Umweg über klassische Gruppenrichtlinien (GPOs). Falls du bestehende GPOs importiert hast, werden viele dieser Einstellungen automatisch übernommen. Der Vorteil der Verwendung dieser spezifischen Policies liegt darin, dass sie gezielt für die Verwaltung der Microsoft 365 Apps entwickelt wurden.



The screenshot shows the Microsoft 365 Apps Policy configuration interface. On the left, a navigation pane lists steps: Basics (checked), Scope (checked), Policies (checked), and Review and publish (unchecked). The main area, titled "Policy", contains the following settings:

- Show Mini Toolbar on selection
- Allow Trusted Locations on the network
- Alternate startup file location
- Automatically Flash Fill **links** (highlighted with a red box)
- Automatically Flash Fill
- Automatically insert a decimal point
- AutoRecover delay
- AutoRecover save location
- AutoRecover time
- Check for accessibility issues while editing
- Block all unmanaged add-ins
- Block macros from running in Office files from the internet
- Block Excel XLL Add-ins that come from an untrusted source
- Allow formatting and labels to track data points

Bild 137: Policies

Bevor du dich der App Protection oder App Configuration widmest, solltest du außerdem einen Blick in den Bereich **Endpoint Security** werfen. Gehe hierzu in Intune auf **Endpoint Security** und dort auf **Security Baselines**. Microsoft stellt dir hier vorgefertigte Konfigurationssätze zur Verfügung, mit denen du Endgeräte aus sicherheitstechnischer Sicht absichern kannst.

Die Security Baselines sind empfohlene Standardkonfigurationen von Microsoft, um Sicherheitslücken zu vermeiden und ein einheitliches Schutzniveau auf Geräten sicherzustellen. Innerhalb Intune stehen dir verschiedene Baselines zur Verfügung, darunter beispielsweise:

- Microsoft Defender for Endpoint
- Microsoft Edge Security Baseline
- Windows 365 Security Baseline
- Microsoft 365 Apps for Enterprise Baseline

Jede dieser Baselines enthält eine Sammlung vordefinierter Richtlinien, die Best Practices für den jeweiligen Anwendungsbereich umsetzen. Du kannst diese Baselines übernehmen und in deiner Umgebung zuweisen, um z. B. sicherzustellen, dass Microsoft Edge abgesichert ist oder dass Defender for Endpoint auf allen Geräten mit definierten Schutzeinstellungen läuft.

Die Kombination aus **App-Schutzrichtlinien**, **Microsoft 365 Application Policies** und **Security Baselines** bietet dir eine umfassende Möglichkeit, deine Endgeräte und Applikationen konsistent zu härten und gleichzeitig sicherzustellen, dass nur verwaltete und konforme Systeme Zugriff auf Unternehmensressourcen erhalten.

Wenn du dich in Intune mit den **Security Baselines** beschäftigst, hast du die Möglichkeit, auf vordefinierte Richtliniensätze von Microsoft zurückzugreifen. Ein Beispiel hierfür ist die Windows 10 Security Baseline. Um diese zu nutzen, gehst du in Intune auf **Endpoint Security**, wählst dort **Security Baselines** und klickst bei „Windows 10 security baseline“ auf **Create Profile**. Nachdem du dem Profil einen Namen vergeben hast, kannst du gezielt Richtlinien konfigurieren.



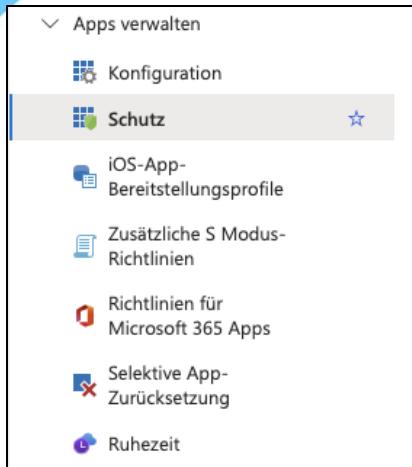
Bild 138: Security Baseline

Ein Blick in die Konfigurationsbereiche, wie z. B. **Browser**, zeigt dir beispielhaft: Der integrierte Passwortmanager ist blockiert, der SmartScreen-Filter aktiviert, „Prevent certificate error override“ ist auf „Enable“ gesetzt. Im Bereich **Microsoft App Store** findest du ebenfalls Einschränkungen, z. B. „Allow game DVR“ auf „Blocked“, „Allow user control over installations“ auf „Disabled“. Dieses vorgefertigte Regelwerk basiert auf Microsoft-Empfehlungen.



Bild 139: Browser Settings

Du solltest jedoch nicht automatisch die gesamte Baseline ungeprüft übernehmen. Es kann dabei zu **Konflikten mit bestehenden Konfigurationen** kommen, was wiederum Zuweisungsprobleme nach sich ziehen kann. Zudem stellt die Microsoft Security Baseline eine **generische Empfehlung** dar, die möglicherweise nicht exakt zu deiner Unternehmensumgebung passt. Daher empfiehlt es sich, jede einzelne Einstellung zu prüfen und daraus ggf. **eigene, angepasste Richtlinienprofile** abzuleiten.



Im Anschluss kannst du dich dem Bereich **App Protection Policies** widmen. Navigiere dazu in Intune unter **Apps > App protection policies**. Solltest du noch keine App Protection Policies angelegt haben, kannst du hier beginnen.

Bild 140: App Schutz

Das Grundprinzip dieser Richtlinien ist, einen **Container** um Unternehmensanwendungen zu legen, der sensible Daten vor ungewolltem Zugriff schützt – insbesondere auf mobilen Plattformen wie **iOS** und **Android**. Auch unter Windows sind App Protection Policies prinzipiell möglich, jedoch derzeit technisch weniger stabil und funktional im Vergleich zu den mobilen Betriebssystemen.

Nach der Vergabe eines Namens für die Richtlinie legst du fest, **welche Applikationen** durch die Richtlinie geschützt werden sollen. Hierzu stehen dir drei Optionen zur Verfügung:

1. All apps
- Es werden alle unterstützten Applikationen einbezogen – sowohl Microsoft- als auch Drittanbieter-Apps wie Adobe oder Azure Information Protection. Eine Liste der betroffenen Applikationen wird dir angezeigt.
2. All Microsoft apps
- Diese Auswahl beschränkt sich auf Microsoft-Anwendungen wie Outlook, OneDrive, Teams, Word, Excel, PowerPoint, Dynamics und Loop.
3. Core Microsoft apps
- Diese Variante fokussiert sich auf die grundlegenden Office-Anwendungen und ist stark reduziert.

i Device type targeting has moved to the Assignments step in policy creation. [Learn more about assigning App Protection Policies](#)

Target policy to

Core Microsoft Apps

i We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

Bild 141: Auswahl der Apps

Durch die Auswahl der betroffenen Applikationen definierst du, welche Programme künftig innerhalb eines geschützten App-Containers laufen. Das hilft dabei, Unternehmensdaten gegen Datenabfluss oder -verlust abzusichern – selbst auf privaten Endgeräten.

Diese Kombination aus angepasster Security Baseline und gezielter App-Schutzrichtlinie ermöglicht es dir, sowohl Endgeräte als auch Anwendungen innerhalb deiner Umgebung umfassend abzusichern.

Wenn du beispielsweise eine Richtlinie für die **Office Suite** konfigurierst – der Prozess ist für andere Applikationen identisch –, gelangst du nach der Auswahl und der Zuordnung der Zielplattformen in den Abschnitt **Data Protection**. Dort legst du fest, wie mit **organisationsbezogenen Daten** innerhalb der verwalteten Apps umgegangen werden darf.

Zunächst gibt es die Einstellung **Backup org data to iTunes and iCloud backups**. Diese bestimmt, ob Daten aus verwalteten Anwendungen in **persönliche Backups**, wie iCloud oder iTunes, aufgenommen werden dürfen. In vielen Szenarien ist es ratsam, diese Option auf **Block** zu setzen, um die unkontrollierte Ablage von Unternehmensdaten in private Cloud-Dienste zu verhindern.

Darauf folgen zwei zentrale Richtlinien zur **Datenübertragung zwischen Applikationen**:

- Send org data to other apps – Hier definierst du, an welche Apps organisationsbezogene Daten weitergegeben werden dürfen.
- Receive data from other apps – Hier legst du fest, von welchen Apps organisationsbezogene Daten empfangen werden dürfen.

In beiden Fällen kannst du verschiedene Freigabemodi konfigurieren:

- Any app – uneingeschränkter Datenversand bzw. -empfang an bzw. von beliebigen Applikationen.
- Policy managed apps – nur an bzw. von Anwendungen, die ebenfalls durch App Protection Policies verwaltet werden.
- Policy managed apps with OS sharing – erlaubt das Teilen bzw. Empfangen von Daten mit ausgewählten OS-Funktionen wie „Öffnen mit“ oder „Teilen über“.
- Block – verhindert vollständig jegliche Kommunikation in der jeweiligen Richtung.

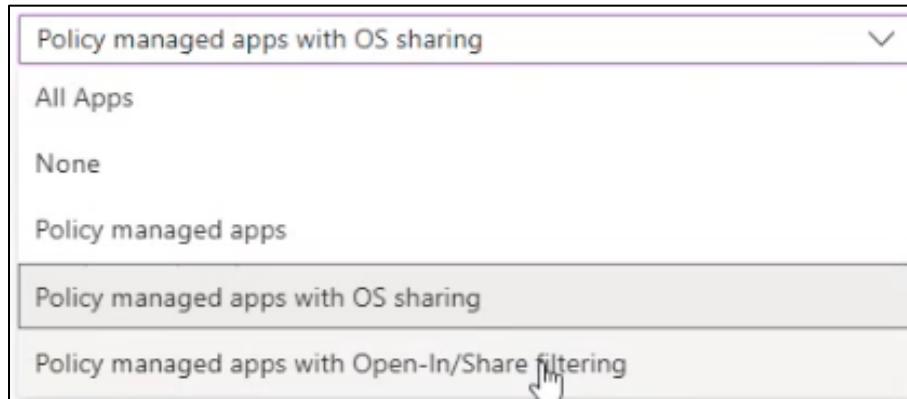


Bild 142: Freigabemodi

Das bedeutet konkret: Möchtest du z. B. verhindern, dass ein Benutzer einen Link aus einer E-Mail in Outlook in einem nicht verwalteten Browser öffnet, solltest du den Datenaustausch ausschließlich auf **Policy managed apps** beschränken.

Darüber hinaus kannst du auch das **Kopieren und Einfügen von Daten** zwischen Anwendungen einschränken. Die Einstellung **Restrict cut, copy, and paste between other apps** regelt genau dies. Hier hast du ebenfalls folgende Auswahlmöglichkeiten:

- Block – Kopieren/Einfügen wird vollständig unterbunden.
- Policy managed apps – erlaubt Copy/Paste nur zwischen verwalteten Anwendungen.
- Policy managed with paste in – erlaubt Einfügen aus anderen Quellen, aber keine Datenweitergabe hinaus.
- Any app – keine Einschränkungen.

Create policy

Backup org data to iTunes and iCloud backups ⓘ	<input checked="" type="radio"/> Allow	<input type="radio"/> Block
Send org data to other apps ⓘ	Policy managed apps with Open-In/Share filtering	
Select apps to exempt	<input type="button" value="Select"/>	
Select universal links to exempt	<input type="button" value="Select"/>	
Select managed universal links	<input type="button" value="Select"/>	
Save copies of org data ⓘ	<input checked="" type="radio"/> Allow	<input type="radio"/> Block
Allow user to save copies to selected services ⓘ	0 selected	
Transfer telecommunication data to ⓘ	Any dialer app	
Dialer App URL Scheme		
Transfer messaging data to ⓘ	Any messaging app	
Messaging App URL Scheme		
Receive data from other apps ⓘ	All Apps	
Open data into Org documents ⓘ	<input checked="" type="radio"/> Allow	<input type="radio"/> Block
Allow users to open data from selected services ⓘ	4 selected	
Restrict cut, copy, and paste between other apps ⓘ	Policy managed apps with paste in	

Bild 143: Create policy

Durch diese granularen Einstellungen stellst du sicher, dass vertrauliche Unternehmensdaten nur innerhalb eines sicheren und kontrollierten Anwendungsrahmens verarbeitet und ausgetauscht werden können. Die Konfiguration der Data Protection-Komponenten ist ein wesentlicher Bestandteil jeder effektiven App Protection Policy.

App Protection Policies – Data Protection und Access Requirements

Die App Protection Policies in Microsoft Intune bieten dir die Möglichkeit, Unternehmensdaten innerhalb mobiler Anwendungen gezielt zu schützen. Sobald du eine solche Richtlinie auf Basis von iOS oder Android erstellst – exemplarisch anhand der Office Suite erklärt –, definierst du im Abschnitt **Data Protection**, wie Daten zwischen Anwendungen verarbeitet und abgesichert werden.

Ein konkreter Effekt dieser Konfiguration ist, dass ein Nutzer z. B. Text aus Microsoft Teams nicht in eine nicht verwaltete App wie WhatsApp einfügen kann. Der kopierte Text wird in diesem Fall ersetzt durch eine Standardmeldung, etwa: „Durch eine Richtlinie Ihres Unternehmens kann dieser Text nicht eingefügt werden.“ Der gleiche Mechanismus funktioniert auch in umgekehrter Richtung – d. h., auch von WhatsApp kann nicht in Teams eingefügt werden. Du kannst hier optional einschränken, ob nur das Kopieren, nur das Einfügen oder beides blockiert werden soll. Ebenso lässt sich ein **Zeichenlimit** für das Kopieren und Einfügen festlegen.

Ein weiterer Punkt betrifft die **Tastaturwahl**. Du kannst festlegen, ob neben der nativen Tastatur des Geräts auch **Drittanbieter-Tastaturen** erlaubt sind. In der Praxis spielt das heute nur noch eine geringe Rolle, da die Nutzung alternativer Tastaturen deutlich zurückgegangen ist.

Die in der Richtlinie enthaltene App wird in einem **verschlüsselten Container** betrieben. Das bedeutet, dass der Zugriff stets verschlüsselt erfolgt. In der Folge kann es zu einem spürbaren Energieverbrauch kommen, da die Verschlüsselung im Hintergrund dauerhaft aktiv ist – laut Microsoft ist dies zwar messbar, aber nicht kritisch.

Ein weiterer zentraler Punkt ist die **Synchronisierung von App-Daten mit nativen Apps**. Du kannst hier entscheiden, ob z. B. geschäftliche Kontakte aus Outlook in die native Kontakte-App des Geräts synchronisiert werden dürfen. Viele Organisationen blockieren das bewusst, um zu verhindern, dass Kontakte in Drittanbieter-Apps wie WhatsApp oder in Anruferanzeigen im Auto erscheinen. Wird die Synchronisation blockiert, erscheinen Anrufer etwa nur mit ihrer Telefonnummer, nicht mit Namen – sofern dieser Kontakt nicht in der privaten Kontaktliste des Geräts enthalten ist.

Darüber hinaus kannst du festlegen, ob Inhalte **gedruckt** werden dürfen oder nicht. Diese Einschränkung bietet eine zusätzliche Maßnahme zur Datenkontrolle.

Data Transfer

Backup org data to iTunes and iCloud backups ⓘ	<input type="button" value="Allow"/> <input type="button" value="Block"/>
Send org data to other apps ⓘ	Policy managed apps with Open-In/Share filtering <input type="button" value="▼"/>
Select apps to exempt <input type="button" value="Select"/>	
Select universal links to exempt <input type="button" value="Select"/>	
Select managed universal links <input type="button" value="Select"/>	
Save copies of org data ⓘ	<input type="button" value="Allow"/> <input type="button" value="Block"/>
Allow user to save copies to selected services ⓘ	<input type="button" value="0 selected"/> <input type="button" value="▼"/>
Transfer telecommunication data to ⓘ	Any dialer app <input type="button" value="▼"/>
Dialer App URL Scheme <input type="button" value="▼"/>	
Transfer messaging data to ⓘ	Any messaging app <input type="button" value="▼"/>
Messaging App URL Scheme <input type="button" value="▼"/>	
Receive data from other apps ⓘ	All Apps <input type="button" value="▼"/>

Bild 144: Data Protection

Im Bereich **Access Requirements** definierst du die Zugriffsvoraussetzungen. Dazu gehört beispielsweise, ob eine **PIN** erforderlich ist, welchen **PIN-Typ** und welche **Komplexität** du zulässt (z. B. einfache oder komplexe PINs mit acht Zeichen). Zudem kannst du biometrische Anmeldeverfahren wie **Touch ID** oder **Face ID** aktivieren. Dabei wird bei der ersten Anmeldung eine PIN gesetzt, die später durch biometrische Verfahren ersetzt werden kann. Du kannst außerdem definieren, **nach wie vielen Minuten Inaktivität** die PIN erneut abgefragt werden soll.

Es ist auch möglich, einen **PIN-Reset** nach einer bestimmten Anzahl von Tagen zu verlangen. Dies wird in der Praxis jedoch häufig vermieden, um die Benutzerfreundlichkeit nicht zu beeinträchtigen.

Ein weiterer Parameter ist die Einstellung „**Work or School Account required**“. Diese Option solltest du auf „**Not required**“ lassen, da sonst bei jedem Zugriff erneut Benutzername und Passwort eingegeben werden müssten – was sich negativ auf die Benutzererfahrung auswirkt.

PIN for access ⓘ	<input checked="" type="button"/> Require	<input type="button"/> Not required
PIN type ⓘ	<input checked="" type="button"/> Numeric	<input type="button"/> Passcode
Simple PIN ⓘ	<input type="button"/> Allow	<input checked="" type="button"/> Block
Select minimum PIN length ⓘ	8	
Touch ID instead of PIN for access (iOS 8+/iPadOS) ⓘ	<input checked="" type="button"/> Allow	<input type="button"/> Block
Override biometrics with PIN after timeout ⓘ	<input checked="" type="button"/> Require	<input type="button"/> Not required
Timeout (minutes of inactivity) *	30	
Face ID instead of PIN for access (iOS 11+/iPadOS) ⓘ	<input checked="" type="button"/> Allow	<input type="button"/> Block
PIN reset after number of days ⓘ	<input type="button"/> Yes	<input checked="" type="button"/> No
Number of days	0	
App PIN when device PIN is set ⓘ	<input checked="" type="button"/> Require	<input type="button"/> Not required
Work or school account credentials for access ⓘ	<input checked="" type="button"/> Require	<input type="button"/> Not required
Recheck the access requirements after (minutes of inactivity) * ⓘ	30	

Bild 145: Access Requirements

Der letzte Abschnitt der Konfiguration behandelt das Thema **Conditional Launch**. Hier wird festgelegt, **unter welchen Bedingungen eine App starten darf** oder nicht. Beispielsweise kannst du festlegen, wie oft ein Nutzer seine PIN falsch eingeben darf, bevor der Zugriff gesperrt wird. Oder wann das Konto entfernt wird, wenn eine Inaktivitätszeit überschritten wird. Auch Bedingungen wie die **mindestens erforderliche App-Version, gerootete oder jailbroken Geräte, bestimmte Betriebssystemversionen** oder sogar spezifische **Modellnummern** können hier als Voraussetzung für den Zugriff definiert werden.

Diese Richtlinien bieten sich insbesondere dann an, wenn du z. B. mit externen Consultants arbeitest. Häufig erhalten externe Mitarbeiter Zugriff auf sensible Daten über mobile Geräte. Anstatt diese Geräte vollständig in die Unternehmensverwaltung zu übernehmen, kannst du mit App Protection Policies gezielt sicherstellen, dass die genutzten Anwendungen geschützt sind und die Unternehmensdaten im Container verbleiben. So lässt sich ein kontrollierter Zugriff auch ohne vollständige Geräteverwaltung sicherstellen.

App conditions

Setting	Value	Action	...
Max PIN attempts	5	Reset PIN	...
Offline grace period	1440	Block access (minutes)	...
Offline grace period	90	Wipe data (days)	...
Disabled account	Select one		...
Select one			

D Jailbroken/rooted devices
 C Min OS version
 S Max OS version
 Device model(s)
 Max allowed device threat level
 Primary MTD service

Value	Action	...
	Block access	...
Select one		

Bild 146: Conditional Launch

Kapitel 31: Applikationsbereitstellung in Microsoft Intune

Zunächst einmal findest du unter dem Bereich **Apps > All Apps** eine Übersicht aller Applikationen, die in deinem Intune-Tenant bereits hinterlegt sind. Wenn du bereits Anwendungen über Intune deployed hast, wirst du dort entsprechende Einträge finden – typischerweise Microsoft 365 Business Apps, Drittanbieter-Tools wie TeamViewer, Starface oder TopDesk sowie Weblinks oder branchenspezifische Applikationen wie eine AusweisApp.

Name ↑	Plattform	Typ	Version
Acrobat Reader	Windows	Windows-App (Win32)	
Acrobat Reader DC	Windows	Windows-App (Win32)	
Adobe Reader DC MSI Test	Windows	Branchenspezifische Wi...	22.3.20322.0
CCleaner	Windows	Branchenspezifische Wi...	5.63.7540
Google Chrome	Android	Verwaltete Google Play ...	
Google Chrome	Windows	Branchenspezifische Wi...	67.228.49268
Intune Company Portal	Android	Verwaltete Google Play ...	
LinkedIn: Jobs & Business News	Android	Verwaltete Google Play ...	
Managed Home Screen	Android	Verwaltete Google Play ...	
Microsoft Authenticator	Android	Verwaltete Google Play ...	
Microsoft Edge für Windows 10	Windows	Microsoft Edge (Windo...	

Bild 147: Übersicht Apps

Beim Anlegen einer App wirst du zunächst gefragt, welchen Applikationstyp du bereitstellen möchtest. Dazu klickst du auf „Erstellen“ und wählst im nächsten Schritt den passenden **App-Typ**. Häufig verwendete Optionen sind etwa:

- iOS Store App
- Android Store App
- Weblink (Windows oder iOS)
- Line-of-Business-App (LOB-App)
- Volume Purchase Program App (für Apple)

Wenn du dich für die Bereitstellung einer **iOS Store App** entscheidest, greifst du auf den öffentlichen Apple App Store zu. Du musst dann manuell die URL zur App angeben sowie die App-spezifischen Metadaten (Name, Beschreibung etc.) einpflegen. Der Nachteil hierbei: Der Benutzer bekommt beim Deployment eine Installationsaufforderung. Diese Aufforderung lässt sich nicht unterdrücken, was im unternehmensweiten Rollout störend wirken kann.

Anders verhält es sich beim **Apple Volume Purchase Program (VPP)**, welches du über den **Apple Business Manager** konfigurierst. Hier kannst du die Apps für Geräte im **Supervised-Modus** direkt installieren – ganz ohne Benutzerinteraktion. Der App-Download erfolgt im Hintergrund. Microsoft Intune greift in diesem Fall auf den verwalteten App-Katalog zu, der über

den Apple Business Manager bereitgestellt wird. Sobald ein Gerät dem Unternehmen zugeordnet ist und im **Supervised-Modus** läuft, solltest du daher bevorzugt mit dem VPP arbeiten.

Wenn du eine App hinzufügst, gibst du einen **Namen**, **Beschreibung**, eine **Kategorie** (z. B. Business) und die **Zielgruppen** an. Letztere erfolgt über Benutzer- oder Gerätegruppen. Der Einsatz von **Gerätegruppen** wird empfohlen – insbesondere dann, wenn du konsistentes Verhalten über iPhones und iPads hinweg gewährleisten möchtest.

Auch **Weblinks** lassen sich als App deklarieren. Diese werden in Form eines Icons auf dem Endgerät angezeigt und öffnen beim Anklicken einen Browserlink. Diese Methode eignet sich vor allem für webbasierte Anwendungen oder firmenspezifische Portale. Weblinks können ebenfalls für Windows oder iOS separat definiert und bereitgestellt werden.

Falls du eine App über den öffentlichen Store bereitstellst, bedenke, dass die App-Zuweisung automatisch eine Nutzerbenachrichtigung erzeugt. Diese kann im Fall des Apple Volume Purchase Program hingegen deaktiviert werden, wodurch der Installationsprozess vollständig im Hintergrund erfolgen kann – ein klarer Vorteil im Rollout größerer Geräteflotten.

Zusammenfassend lässt sich festhalten: Für Unternehmen mit verwalteten Geräten, insbesondere im **Supervised-Modus**, ist die Nutzung des **Volume Purchase Program** über den **Apple Business Manager** die bevorzugte Methode. Für Szenarien ohne VPP oder ohne Gerätemanagement ist die Bereitstellung über den öffentlichen Store oder über Weblinks weiterhin möglich, jedoch mit Einschränkungen in der Benutzerfreundlichkeit.

Die App-Bereitstellung in Intune ist modular und flexibel – allerdings empfiehlt es sich, die jeweiligen Geräteeigenschaften sowie den Gerätezustand (z. B. supervision status) bei der Auswahl der Methode sorgfältig zu berücksichtigen.

Erweiterte Applikationsverwaltung mit Apple VPP und Microsoft Store in Intune

Um Applikationen unter iOS und Windows effizient mit Intune bereitzustellen, solltest du dich mit den verfügbaren Bereitstellungsmethoden vertraut machen.

Zunächst überprüfst du, ob euer **Apple VPP Token** bereits in Intune eingebunden ist. Dazu navigierst du in Intune zu **Mandantenverwaltung > Connectors und Tokens** und suchst dort den **Apple Volume Purchase Program (VPP) Connector**.



Bild 148: Apple VPP

Wenn dieser noch nicht verbunden ist, musst du ihn unbedingt hinzufügen. Erst dann werden die Applikationen, die im **Apple Business Manager (ABM)** stehen, automatisch mit Intune synchronisiert. Auf Basis dieser Synchronisierung kannst du dann Apps zentral und ohne Benutzerinteraktion bereitstellen – ein deutlicher Vorteil gegenüber der manuellen Verteilung über den App Store.

Im nächsten Schritt wechselst du zu **Apps > Alle Apps** und klickst auf **Erstellen**, um eine neue App bereitzustellen. Bei iOS unterscheidest du hier zwischen folgenden Typen:

- iOS Store App: Öffentliche Apps aus dem Apple App Store.
- Weblink (ehemals Webclip): Eine URL, die als Icon auf dem Homescreen erscheint.
- Integrierte App: Microsoft-spezifische Systemanwendungen.
- Branchenspezifische App: Anwendungen, die über Formate wie .msi oder .msix bereitgestellt werden (vorwiegend relevant im Windows-Kontext).

Die Bereitstellung über das VPP bietet zusätzliche Vorteile: Automatische Updates, Hintergrundinstallation auf Geräten im **Supervised Mode** und die Möglichkeit, Apps zentral zu verwalten. Du solltest daher bei Geräten im Supervised Mode bevorzugt das VPP nutzen. Nur wenn keine VPP-Integration möglich ist, solltest du auf den öffentlichen App Store zurückgreifen.

Für Android Enterprise Geräte gilt: **Verwende ausschließlich den verwalteten Google Play Store**. Der Zugriff auf den öffentlichen Play Store sollte vermieden werden. Alle notwendigen Anwendungen kannst du über den verwalteten Store definieren und ausrollen.

Für Windows-Systeme hat Microsoft mit dem neuen **Microsoft Store App-Modell** einen ähnlichen Weg eingeschlagen. Dabei findest du im Microsoft Store nicht nur UWP-Anwendungen (Universal Windows Platform), sondern zunehmend auch paketierte **Win32-Anwendungen**, die direkt über Intune ausgerollt werden können. Beispielsweise können hier Anwendungen wie **Adobe Creative Cloud** oder **Adobe Acrobat Reader** über die integrierte Store-Suche gefunden und zugewiesen werden. Dabei siehst du bei der Auswahl, ob es sich um eine UWP-App oder um eine Win32-App handelt. Die Win32-Apps sind bereits durch Microsoft paketiert und können direkt verwendet werden – ein Vorteil, der dir das manuelle Paketieren erspart.

Diese Store-basierten Apps aktualisieren sich automatisch, was die Wartung vereinfacht. Der Einsatz von manuell hochgeladenen Win32-Paketen (z. B. über die Intune-Win32-App-Erstellung) ist in vielen Fällen nicht mehr erforderlich, wenn die App bereits im Store verfügbar ist.

Zusammenfassend empfiehlt sich für die Applikationsverteilung folgende Priorisierung:

1. Apple Volume Purchase Program (bei iOS-Geräten im Supervised-Modus)
2. Microsoft Store (bei Windows 10/11 Geräten)
3. Verwalteter Google Play Store (bei Android Enterprise Geräten)
4. Öffentlicher App Store (nur bei Bedarf)
5. Weblinks (z. B. für webbasierte Anwendungen)
6. Branchenspezifische Apps oder LOB-Apps (.msi, .msix, .intunewin)

Office App-Suite Bereitstellung mit Intune: Konfiguration über den Designer oder XML

Das, was du in Intune siehst, ist funktional das Pendant zum Office Deployment Toolkit – speziell zur Bereitstellung der Office App Suite. Nach der Auswahl der App Suite bekommst du zunächst allgemeine Informationen wie Name, Beschreibung, Herausgeber, Logo und URL angezeigt. Diese Daten kannst du bei Bedarf anpassen.

Informationen zur App-Suite	App-Suite konfigurieren	Zuweisungen	Überprüfen und erstellen
Name der Suite *	Microsoft 365 Apps für Windows 10 und höher		
Beschreibung *	<p>Hilfe zu Markdown erhalten, das für Beschreibungen unterstützt wird.</p> <p>Microsoft 365 Apps für Windows 10 und höher</p>		
	Preview	Microsoft 365 Apps für Windows 10 und höher	
Herausgeber	Microsoft		
Kategorie	Produktivität		
Diese App als ausgewählte App im Unternehmensportal anzeigen	<input type="radio"/> Ja <input checked="" type="radio"/> Nein		
Informations-URL	https://products.office.com/explore-office-for-home		
URL zu den Datenschutzbestimmungen	https://privacy.microsoft.com/privacystatement		
Entwickler	Microsoft		
Besitzer	Microsoft		
Hinweise			
Logo	Bild ändern 		

Bild 149: Informationen Office Suite

Im nächsten Schritt gelangst du über „Weiter“ zur **Konfiguration der App Suite**. Hier stehen dir zwei Methoden zur Auswahl:

1. Konfigurationsdesigner (No-Code-Ansatz)
2. Enter XML (manuelle XML-Eingabe)

Beide Wege führen zum Ziel, unterscheiden sich aber im Detail:

- Die XML-Methode erlaubt eine umfassendere Konfiguration, da sie sich direkt an die Logik des Office Deployment Toolkits anlehnt. Bestehende XML-Dateien aus dem ODT lassen sich hier problemlos einfügen und verwenden – die Kompatibilität ist gegeben.
- Der Konfigurationsdesigner ist hingegen ein visuell geführter, vereinfachter Ansatz (Stichwort: „No brainer“), bei dem du Schritt für Schritt durch die Einstellungen geführt wirst.

Wenn du dich für den Designer entscheidest, klickst du innerhalb der App-Suite-Konfiguration oben auf den Reiter „**Konfigurationsdesigner**“. Dort wählst du im Dropdown bei „XML Daten“ den Punkt „**„Apps Suite konfigurieren – Office Apps auswählen“** aus.

Anschließend legst du fest, **welche Office-Komponenten du bereitstellen möchtest:**

- Word
- Excel
- PowerPoint
- Outlook
- OneNote
- Teams
- Publisher
- Access

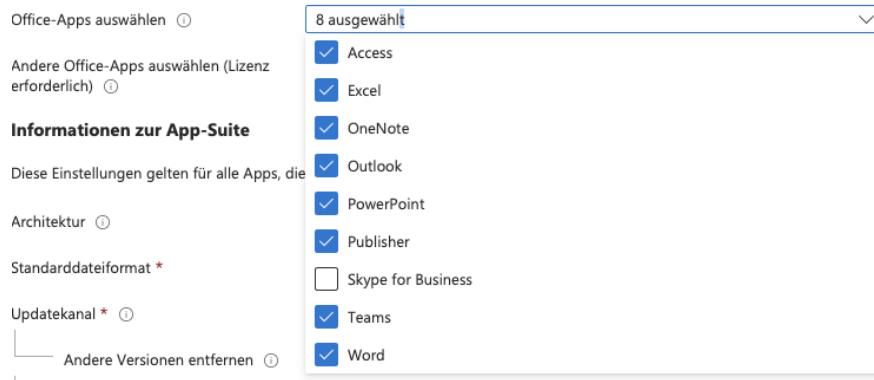


Bild 150: Office Apps auswählen

Du kannst hier gezielt Anwendungen abwählen, die nicht benötigt werden. Häufige Kandidaten für die Abwahl sind z. B. **Access** und **Publisher**, da diese in vielen Umgebungen nicht erforderlich sind.

Diese Vorgehensweise erlaubt dir eine flexible und zentral verwaltete Office-Bereitstellung über Intune – abgestimmt auf die tatsächlichen Anforderungen deiner Umgebung.

Feinkonfiguration der Office App-Suite in Intune: Optionen, Versionen und Sprachpakete

Nachdem du die gewünschten Office-Komponenten ausgewählt hast, kannst du durch einfaches Entfernen einzelner Haken bestimmte Apps wie Access oder Publisher ausklammern – damit ist der Schritt bereits erledigt. Unterhalb dieser Optionen findest du die Auswahl „**Andere Office-Apps**“, worunter z. B. lokale Installationen von **Project Online Desktopclient** und **Visio Online Plan 2** fallen.

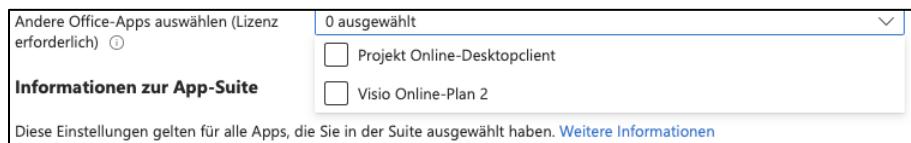


Bild 151: Weitere Office Apps

Auch hier gilt: Wenn die Anwendung ausgewählt wird, aber dem Benutzer keine Lizenz zugewiesen ist, erscheint beim Start lediglich der Hinweis, dass eine gültige Lizenz erforderlich ist – genutzt werden kann sie dann aber nicht.

Ein weiterer wichtiger Abschnitt betrifft die **Allgemeinen Suite-Einstellungen**. Dazu gehören:

- Architektur (32- oder 64-Bit)
- Standarddateiformat, also ob Office-Dateien standardmäßig im XML-Format (docx, xlsx usw.) oder im Open Document Format (ODF) gespeichert werden sollen
→ Diese Auswahl wird durch die IT zentral getroffen, sodass Benutzer dies nicht mehr manuell setzen müssen.

Update-Kanal:

Die Wahl des richtigen Update-Kanals ist entscheidend für Stabilität und Aktualität im Unternehmen. Zur Verfügung stehen unter anderem:

Monatlicher Enterprise-Kanal (empfohlen für Unternehmen)

Aktueller Kanal (entspricht dem öffentlichen Consumer-Release)

Halbjährlicher Enterprise-Kanal (für besonders konservative Update-Zyklen)



Bild 152: Updatekanal

Weitere sinnvolle Optionen unterhalb des Update-Kanals:

Andere Versionen entfernen: Falls das Gerät z. B. per Autopilot mit einer bestehenden Office-Version ausgeliefert wird, kann diese automatisch erkannt, deinstalliert und durch die verwaltete Version ersetzt werden.

Version auswählen: Standardmäßig wird die neueste Version installiert. Du kannst aber auch gezielt eine ältere Version definieren – je nachdem, was Microsoft aktuell zur Verfügung stellt (die Liste variiert regelmäßig).

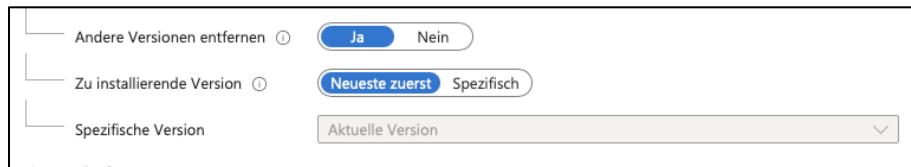


Bild 153: Andere Versionen

Weitere Konfigurationspunkte:

- Aktivierung gemeinsam genutzter Computer (Shared PC Mode)
→ Sinnvoll für Szenarien mit wechselnden Benutzern.
- Automatische Akzeptanz der Lizenzbedingungen
→ Spart Endbenutzern unnötige Interaktionen.
- Microsoft Search-Dienste
→ Diese Funktion ist optional. Viele nutzen sie unbewusst, z. B. für Zusatzinformationen wie Wetteranzeigen oder integrierte Web-Suchdienste in Office.

Sprachpakete in Office:

Standardmäßig wird Office in der primären Sprache des Betriebssystems installiert. Benötigst du zusätzliche Sprachen, kannst du diese gezielt hinzufügen. Dabei stellt sich häufig die Frage nach der richtigen Strategie:

- Eine Suite mit allen Sprachen?
- Mehrere Suiten mit jeweils einzelnen Sprachpaketen?

Hier gibt es kein „richtig“ oder „falsch“. Die Sprachpakete sind allerdings **datenintensiv**, was vor allem in Autopilot-Szenarien zu spürbaren Verzögerungen führen kann. Aus Praxissicht empfiehlt es sich, mit einem sinnvollen Grundstock zu starten und bei wachsendem Bedarf gezielt neue Suiten für zusätzliche Sprachen zu erstellen – **nicht direkt zehn Sprachen in ein einziges Paket integrieren**.

Zuweisung und Bereitstellung von Applikationen in Intune: Grundlagen und Besonderheiten

In Intune folgt die Bereitstellung von Applikationen einem konsistenten Schema, das du bei nahezu jeder App wiederfinden wirst. Typischerweise arbeitest du mit drei **Zuweisungstypen**:

1. **Automatische Installation**
→ Die App wird auf allen zugewiesenen Geräten ohne Benutzerinteraktion installiert. Eine Deinstallation durch den Benutzer ist nicht vorgesehen.
2. **Verfügbar für registrierte Geräte**
→ Die App erscheint im **Unternehmensportal** und kann dort vom Benutzer installiert und auch wieder deinstalliert werden.
3. **Deinstallationszuweisung**
→ Hierbei wird die App gezielt entfernt, sofern sie auf dem Gerät vorhanden ist.

Erforderlich ⓘ	
Gruppenmodus	Gruppe
Keine Zuweisungen	
+ Gruppe hinzufügen ⓘ + Alle Benutzer hinzufügen ⓘ + Alle Geräte hinzufügen ⓘ	
Für registrierte Geräte verfügbar ⓘ	
Gruppenmodus	Gruppe
Keine Zuweisungen	
+ Gruppe hinzufügen ⓘ + Alle Benutzer hinzufügen ⓘ	
Deinstallieren ⓘ	
Gruppenmodus	Gruppe
Keine Zuweisungen	

Bild 154: Zuweisung

Bei der Auswahl, **ob Benutzer oder Geräte zugewiesen werden sollen**, empfiehlt Microsoft, vor allem **Gerätegruppen** zu verwenden – insbesondere bei Richtlinien. In manchen Szenarien kann jedoch auch eine Zuweisung auf **Benutzerebene** sinnvoll sein. Ein Beispiel dafür: Produktions- oder Lagermitarbeiter, die sich flexibel an unterschiedlichen Clients anmelden. In diesem Fall sorgt die Benutzerzuweisung dafür, dass die App **unabhängig vom Gerät** zur Verfügung steht – allerdings gilt es zu beachten, dass die **Installationszeit** pro Gerät trotzdem abgewartet werden muss.

In der App-Übersicht kannst du unter „**Alle Apps**“ > „**Erstellen**“ eine neue Anwendung hinzufügen. Beim Apptyp findest du u. a. die Auswahl „**Microsoft Edge**“, die besonders simpel zu konfigurieren ist:

- **Name, Beschreibung, Herausgeber** werden – soweit möglich – automatisch von Intune vorausgefüllt.
- Danach wählst du den gewünschten **Release-Kanal** (z. B. Stable, Beta, Dev).
- Optional: Festlegung der **Sprache** (Betriebssystemsprache oder manuelle Auswahl).
- Abschließend erfolgt wieder die Zuweisung wie oben beschrieben.

Auch wenn Edge heute meist bereits vorinstalliert ist, geht es hier um die Bereitstellung als **verwaltete Version** – z. B. zur Durchsetzung spezifischer Richtlinien.

① App-Informationen ② App-Einstellungen ③ Zuweisungen ④ Überprüfen und erstellen

Name *	<input type="text" value="Microsoft Edge für Windows 10 und höher"/>
Beschreibung *	<small>Hilfe zu Markdown erhalten, das für Beschreibungen unterstützt wird.</small> <input type="text" value="Microsoft Edge ist der Browser für Unternehmen mit moderner und Legacy-Webkompatibilität, neuen Datenschutzfeatures wie z. B. Nachverfolgungsschutz sowie integrierten Produktivitätstools wie PDF-Unterstützung auf Unternehmenniveau und Zutriff auf Office und die Unternehmenssuche direkt"/>
Preview	<small>Microsoft Edge ist der Browser für Unternehmen mit moderner und Legacy-Webkompatibilität, neuen Datenschutzfeatures wie z. B. Nachverfolgungsschutz sowie integrierten Produktivitätstools wie PDF-Unterstützung auf Unternehmenniveau und Zutriff auf Office und die Unternehmenssuche direkt</small> <input type="text" value="Microsoft Edge ist der Browser für Unternehmen mit moderner und Legacy-Webkompatibilität, neuen Datenschutzfeatures wie z. B. Nachverfolgungsschutz sowie integrierten Produktivitätstools wie PDF-Unterstützung auf Unternehmenniveau und Zutriff auf Office und die Unternehmenssuche direkt"/>
Herausgeber	<input type="text" value="Microsoft"/>
Kategorie	<input type="text" value="Produktivität"/> ▼
Diese App als ausgewählte App im Unternehmensportal anzeigen	<input type="radio" value="Ja"/> <input checked="" type="radio" value="Nein"/>
Informations-URL	<input type="text" value="https://www.microsoft.com/windows/microsoft-edge"/>
URL zu den Datenschutzbestimmungen	<input type="text" value="https://privacy.microsoft.com/privacystatement"/>
Entwickler	<input type="text" value="Microsoft"/>
Besitzer	<input type="text"/>
Hinweise	<input type="text"/>

Bild 155: Microsoft Edge

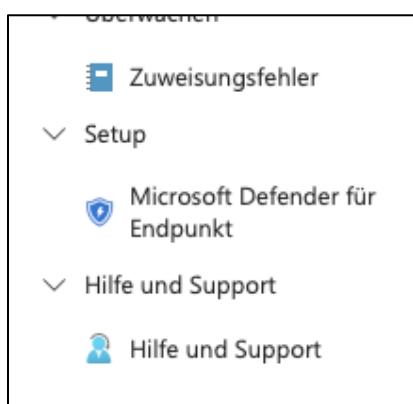
Sonderfall: Microsoft Defender für Endpoint

Für macOS-Geräte kann **Microsoft Defender für Endpoint** direkt über die App-Bereitstellung in Intune hinzugefügt werden. Dort findest du ihn unter den App-Typen – auch wenn die Menüführung nicht unbedingt intuitiv ist.



Bild 156: Microsoft Defender macOS

Für **Windows-Geräte** hingegen funktioniert das anders: Hier musst du über den linken



Menüpunkt „**Endpunktsicherheit**“ gehen. Am unteren Ende findest du die Option „**Setup Microsoft Defender for Endpoint**“, die dich zur weiteren Konfiguration führt.

Bild 157: Defender Windows

Diese Einstellungen werden über das Portal security.microsoft.com vorgenommen – das auch direkt aus dem Microsoft 365 Admin Center erreichbar ist. Trotz der Vielzahl an Portalen bleibt die Funktionalität dieselbe, auch wenn die Übersichtlichkeit manchmal leidet.

Im Microsoft 365 Security Center lässt sich unter **Settings > Endpoints** der Bereich **Device Management Onboarding** aufrufen. Hier kann man gezielt Windows-10- und Windows-11-Geräte per **Mobile Device Management (MDM)** – in diesem Fall über **Microsoft Intune** – onboarden.

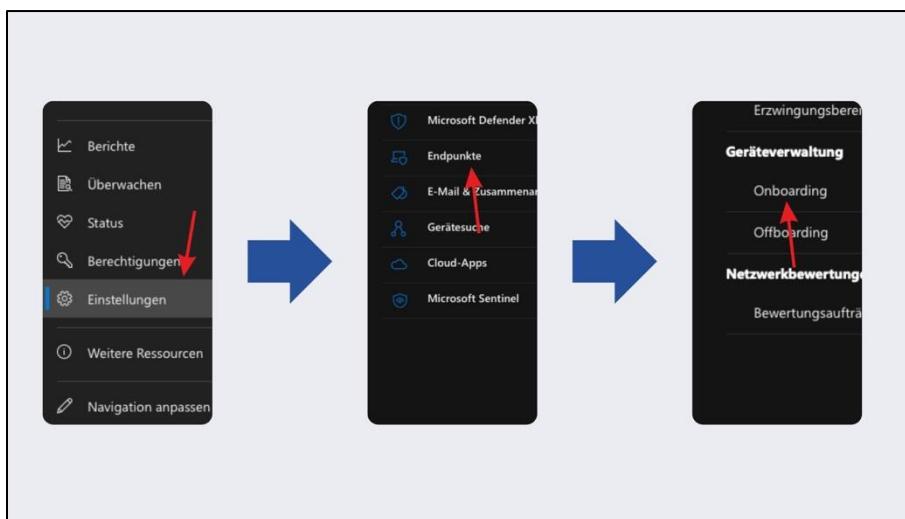


Bild 158: Defender Onboarding

Dafür wird ein entsprechendes **Onboarding-Paket** heruntergeladen, das anschließend in Intune wieder hochgeladen und auf die Geräte verteilt wird. Diese Geräte erscheinen nach erfolgreichem Onboarding im Bereich **Assets > Devices**, wo sie fortan überwacht und verwaltet werden können.

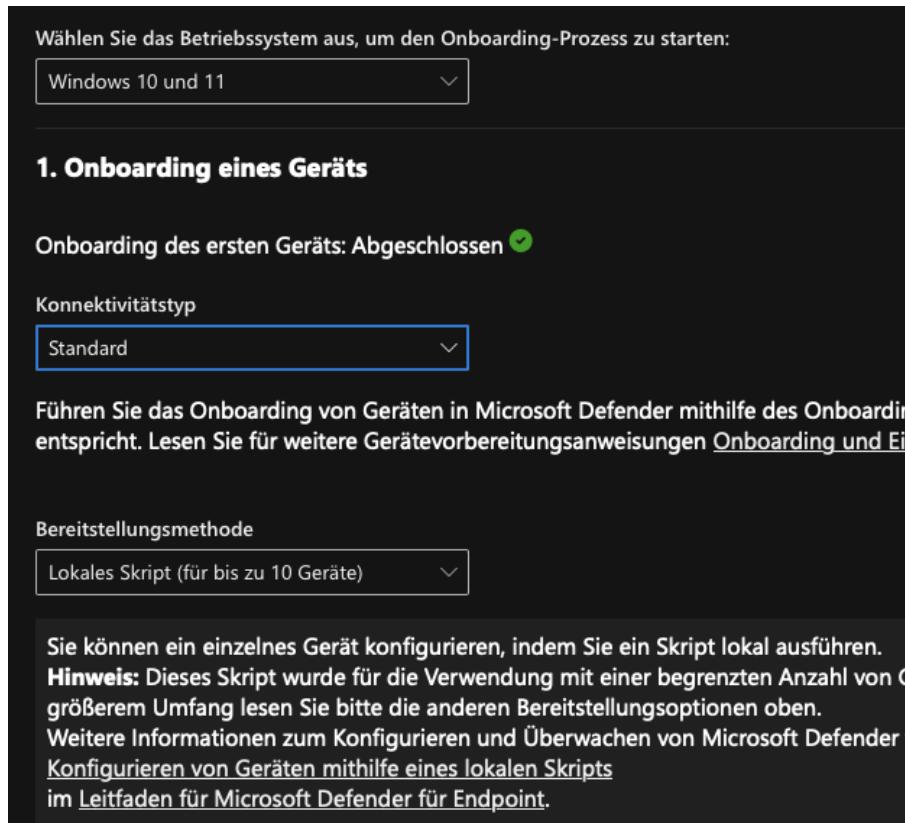


Bild 159: Onboarding-Paket

Nach dem Onboarding erhalten Administratoren tiefgehende Einblicke in die einzelnen Geräte. Beispielsweise wird sichtbar, welche **Benutzer sich zuletzt angemeldet haben**, welches **Exposure Level** das Gerät aktuell hat, und es werden **automatische Empfehlungen** gegeben – etwa zur Aktualisierung installierter Programme wie Google Chrome, Visual Studio oder Mozilla Thunderbird, oder zur Anpassung von Passwortlängen. Der Defender inventarisiert zudem alle relevanten Informationen, sammelt bei Bedarf Incident-Alerts und bietet so ein zentrales Monitoring-Tool.

Gleichzeitig sollte man sich bewusst sein, dass diese Funktionalitäten die **Transparenz über das Nutzungsverhalten** stark erhöhen. Mit Defender lassen sich theoretisch alle Anwendungen, Dateien und sogar **besuchte Webseiten** nachvollziehen. Auch wenn das primär der Sicherheit dient, wirft es datenschutzrechtlich kritische Fragen auf – besonders im deutschen Kontext.

Ein weiterer relevanter Punkt im Security Center ist **Cloud Apps / Cloud Discovery**. Sobald Geräte geonboardet sind und Defender for Endpoint aktiv ist, kann über diesen Bereich eingesehen werden, **welche Applikationen und Dienste** im Unternehmen tatsächlich verwendet werden. Die Analyse erfolgt rückblickend auf einen Zeitraum von 30 Tagen. Dabei werden Applikationen wie z. B. YouTube, deren Datenvolumen oder Nutzungshäufigkeit automatisch erfasst. Auch wenn diese Informationen unterschiedlich interpretiert werden können, bietet die Übersicht eine wertvolle Grundlage zur Bewertung und Kategorisierung der eingesetzten Software.

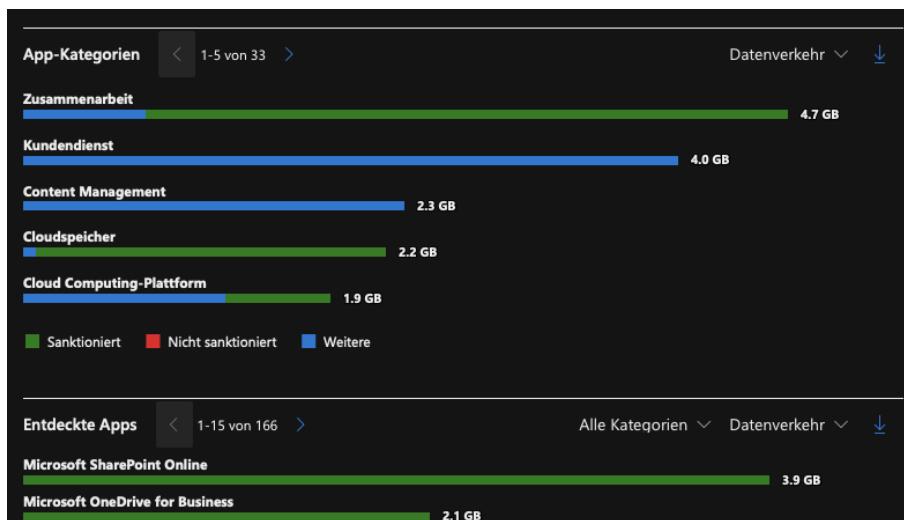


Bild 160: Cloud Discovery

Über **Cloud Discovery** können Administratoren festlegen, welche Anwendungen **freigegeben**, welche **noch zu validieren** oder potenziell **abzulehnen** sind. Das System unterscheidet dabei nicht nur zwischen klassischen Anwendungen, sondern auch **SaaS-Diensten**, **Hintergrundprozessen**, **Webseiten** und vielem mehr. Jede Applikation erhält zudem einen **Risk Score**, der durch Kriterien wie Funktionalität, Sicherheitsfeatures und allgemeine Bekanntheit beeinflusst wird. Über eine Detailansicht wie **View Score Breakdown** lassen sich diese Bewertungen nachvollziehen – zum Beispiel bei weniger bekannten Anwendungen. Wenn ein

Tool bestimmte Sicherheitsfunktionen nicht bietet oder sich nicht eindeutig dazu äußert, wirkt sich das negativ auf die Gesamtbewertung aus.



Bild 161: Bewertung der App

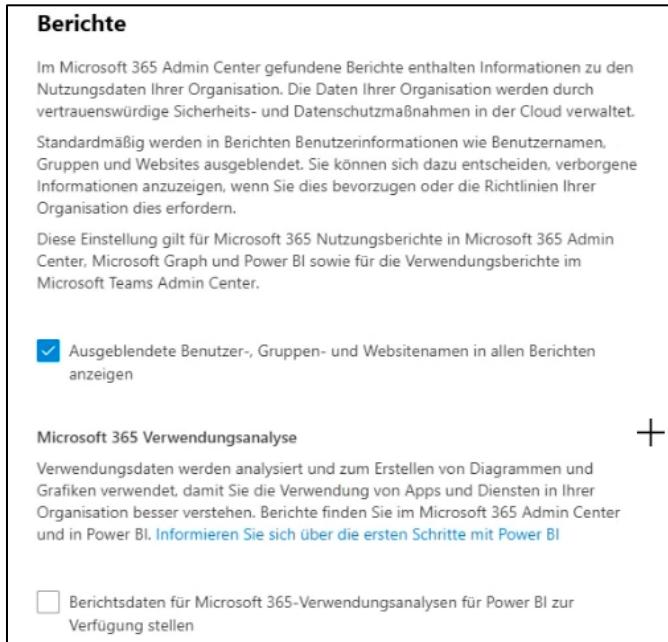
Ergänzend dazu lassen sich im Rahmen der Sicherheitskonfiguration auch Einstellungen wie **App Protection Policies** mit evaluieren. Innerhalb einer Business Premium Lizenz erhält man in Kombination mit dem Security Center, Intune, Conditional Access und weiteren Funktionen ein leistungsstarkes Gesamtpaket – einschließlich moderner Endpoint Protection und MDM – das eine umfassende Steuerung und Absicherung der Geräteflotte ermöglicht.

Im Microsoft Defender for Endpoint gibt es eine umfassende **Compliance-Bewertung**, die nicht nur technische Kriterien, sondern auch rechtliche Aspekte berücksichtigt. Aaron weist jedoch darauf hin, dass diese Bewertungen mit Vorsicht zu genießen sind – insbesondere, weil Microsoft-eigene Dienste naturgemäß sehr gute Scores erhalten. Diese **Eigenbewertung innerhalb der Microsoft-Welt** sollte man kritisch betrachten. Dennoch bietet das Tool eine sinnvolle Grundlage, um zu verstehen, welche Anwendungen im Unternehmen tatsächlich genutzt werden – insbesondere im Kontext von **Schatten-IT**.

Im Vergleich zu den Basisfunktionen, die bereits in **Entra ID** vorhanden sind, handelt es sich hierbei um eine **erweiterte Analyseplattform**. Beispielsweise lassen sich Anwendungen wie **Instagram** oder **Netflix** identifizieren und auswerten. Für jede erkannte App wird erfasst, **wie viele Benutzer** sie aktuell nutzen, **wie viel Traffic sie erzeugt**, sowie über welche **IP-Adressen** der Zugriff erfolgt. Der Nutzungsverlauf lässt sich über mehrere Wochen hinweg

verfolgen, inklusive eines **Top-Rankings** nach Datenvolumen. Überraschend war in der Schulung etwa, dass Netflix in einem Fall sogar freigegeben war.

Wichtig ist: Die erfassten **Klarnamen** der Nutzer lassen sich auf Wunsch **pseudonymisieren**. In den **Organisationseinstellungen unter dem Punkt „Berichte“** besteht die Möglichkeit, personenbezogene Daten auszublenden. Das ist insbesondere im Hinblick auf Datenschutz und DSGVO ein relevanter Hinweis.



Berichte

Im Microsoft 365 Admin Center gefundene Berichte enthalten Informationen zu den Nutzungsdaten Ihrer Organisation. Die Daten Ihrer Organisation werden durch vertrauenswürdige Sicherheits- und Datenschutzmaßnahmen in der Cloud verwaltet.

Standardmäßig werden in Berichten Benutzerinformationen wie Benutzernamen, Gruppen und Websites ausgeblendet. Sie können sich dazu entscheiden, verborgene Informationen anzuzeigen, wenn Sie dies bevorzugen oder die Richtlinien Ihrer Organisation dies erfordern.

Diese Einstellung gilt für Microsoft 365 Nutzungsberichte in Microsoft 365 Admin Center, Microsoft Graph und Power BI sowie für die Verwendungsberichte im Microsoft Teams Admin Center.

Ausgeblendete Benutzer-, Gruppen- und Websitenamen in allen Berichten anzeigen

Microsoft 365 Verwendungsanalyse

Verwendungsdaten werden analysiert und zum Erstellen von Diagrammen und Grafiken verwendet, damit Sie die Verwendung von Apps und Diensten in Ihrer Organisation besser verstehen. Berichte finden Sie im Microsoft 365 Admin Center und in Power BI. [Informieren Sie sich über die ersten Schritte mit Power BI](#)

Berichtsdaten für Microsoft 365-Verwendungsanalysen für Power BI zur Verfügung stellen

Bild 162: Berichte

In diesem Zusammenhang kam die Frage auf, ob sich auch **Apps deinstallieren lassen**, die **nicht zentral über Intune** bereitgestellt wurden – also z. B. durch den Benutzer selbst installiert wurden. Aaron erklärt, dass es **keinen direkten Intune-Befehl** gibt, der solche Apps automatisch entfernt.

Es existieren jedoch **Community-gestützte Lösungen**, etwa das sogenannte **General Uninstaller Script**, mit dem sich Applikationen anhand ihres **Produktnamens** identifizieren und anschließend deinstallieren lassen. Dieses Skript kann individuell angepasst, paketiert und über Intune verteilt werden.

Eine weitere Möglichkeit stellt der **MS.Manager** dar, ein Tool von **Cloud and Cover**, das speziell für den Umgang mit **Built-in Apps** entwickelt wurde. Hierüber können z. B. auch herstellerspezifische Bloatware wie **Lenovo Vantage** oder andere vorinstallierte Programme entfernt werden. Besonders bei Geräten von Lenovo oder Dell, die oft mit zahlreichen Zusatzttools ausgeliefert werden, kann das relevant sein. Aaron berichtet aus eigener Erfahrung, dass Lenovo für ein „sauberes Image“ teilweise bis zu 50 € pro Gerät verlangt – eine Kostenfalle, die sich durch den Einsatz dieser Skripte vermeiden lässt.

Beschäftige dich mit dem **MS.Manager Blog** zu beschäftigen, da dieser regelmäßig nützliche Skripte und Anleitungen für die App-Verwaltung bereitstellt – gerade auch im Kontext von Gerätebereitstellungen, Bloatware-Entfernung und benutzerseitig installierter Software.

Kapitel 32 – MSI- und Win32-App-Deployment mit Microsoft Intune

Zunächst ist es wichtig zu wissen, dass du **MSI-Dateien** grundsätzlich direkt in Intune hochladen kannst. Das System erkennt diese Installationspakete und kann sie entsprechend verarbeiten. Allerdings wird von Microsoft empfohlen, nicht direkt mit reinen MSI-Dateien zu arbeiten, sondern diese vor dem Deployment in das **Intune-WIN-Format** zu konvertieren. Dieses Format ist speziell für Intune optimiert und bietet dir mehr Flexibilität bei der App-Paketierung und -Verteilung. Es handelt sich hierbei um das bevorzugte Format, mit dem du auch später im Alltag arbeiten solltest.

Zuerst geht es darum Anwendungen in das Intune-WIN-Format zu bringen und über das Endpoint Manager Admin Center zu verteilen. Dabei ist es unerlässlich, das richtige Tool zur Umwandlung in das WIN-Format zu verwenden – nämlich das „Microsoft Win32 Content Prep Tool“. Mit diesem Tool wandelst du deine Setup-Dateien, also z. B. eine MSI-Datei oder ein komplettes Installationsverzeichnis, in ein Intune WIN-Format um. Dieses Paket wird anschließend in Intune hochgeladen und als Applikation bereitgestellt.

Der Vorteil dieser Methode ist nicht nur die einheitliche Verarbeitung innerhalb von Intune, sondern auch die Möglichkeit, komplexere Installationslogik zu definieren – etwa durch benutzerdefinierte Befehle oder zusätzliche Parameter. Gerade wenn du mehrere

Anwendungen gleichzeitig oder in einer bestimmten Reihenfolge installieren möchtest, ist das Intune-WIN-Format deutlich flexibler als die direkte MSI-Variante.

Jede Organisation hat unterschiedliche Anforderungen. Deshalb solltest du beim App Deployment stets prüfen, ob es spezifische Vorgaben oder Besonderheiten in deiner Umgebung gibt – etwa bei der Benutzerinteraktion, bei Rechten oder im Zusammenspiel mit Conditional Access Policies.

Auswahl des Apptyps im Intune-Portal

Im Rahmen des App-Deployments mit Microsoft Intune befindest du dich zunächst im Bereich **Apps**. Dort wählst du die Option „**Create**“ auf der linken Seite aus, um eine neue Anwendung hinzuzufügen. Anschließend wirst du nach dem **Apptypen** gefragt. Für Windows-Systeme stehen dir hier zwei zentrale Möglichkeiten zur Verfügung: *Windows App (Win32)* sowie *Line-of-Business App*.

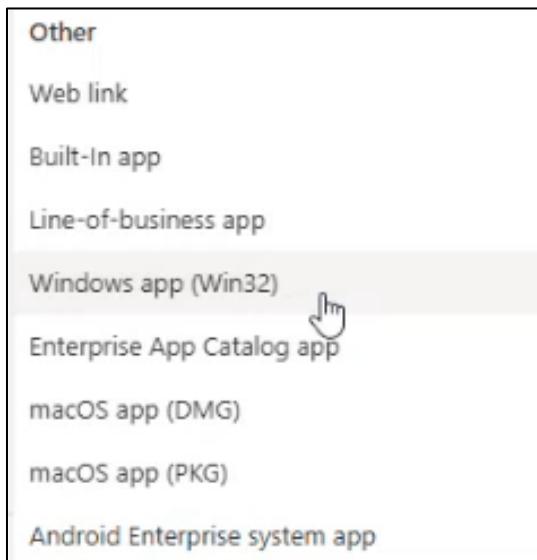


Bild 163: Apptypen Windows

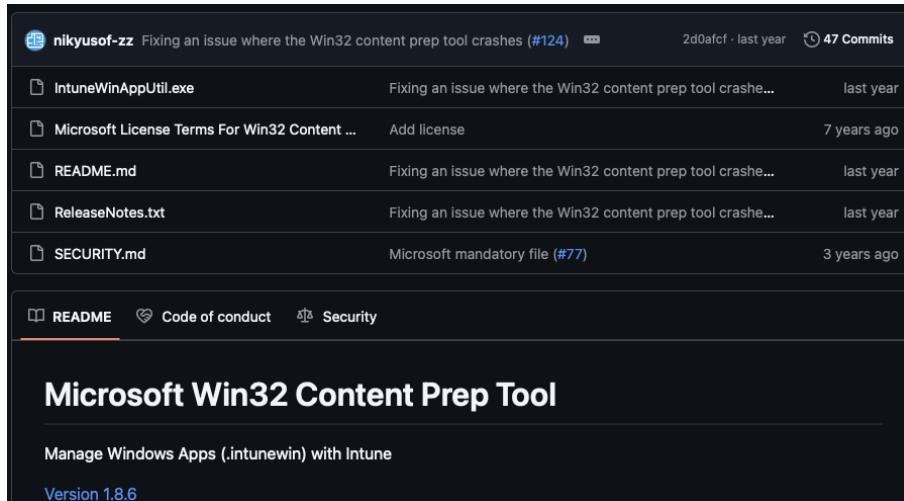
Die sogenannte **Line-of-Business App** erlaubt es dir, ein klassisches MSI-Paket direkt in Intune hochzuladen. Von dieser Variante wird jedoch abgeraten. Auch wenn sie technisch weiterhin

unterstützt wird, empfiehlt Microsoft, auf das **Intune-WIN-Format** zu setzen. Der Grund liegt in der technischen Architektur: MSI-Installationen laufen sequenziell ab, das heißt, sie können nicht parallel zu anderen MSI-Prozessen ausgeführt werden. Dies stellt insbesondere im Kontext von **AutoPilot** ein Problem dar, da dort mehrere Installationen gleichzeitig angestoßen werden können. Eine parallele Ausführung lässt sich in diesem Szenario nicht verhindern, was wiederum zu Installationsfehlern führen kann. Aus diesem Grund weist Microsoft auf der eigenen Learn-Plattform explizit darauf hin, dass **MSI- und Intune-WIN-Dateien nicht miteinander kombiniert** werden sollen.

Ein weiterer Vorteil des Intune-WIN-Formats ist die deutlich höhere Anzahl an verfügbaren **Konfigurationsoptionen**. Du erhältst damit ein flexibleres und besser steuerbares Deployment. Ein Nachteil dieses Formats ist jedoch, dass **kein automatischer Update-Mechanismus** enthalten ist. Wenn du Applikationen auf dem aktuellen Stand halten möchtest, musst du Updates manuell einpflegen und neu paketieren. Im Gegensatz dazu bieten einige MSI-basierte Installationen – sofern die jeweilige Anwendung dies unterstützt – einen eingebauten Auto-Update-Prozess. Ob das ein Vorteil oder Nachteil ist, hängt letztlich von der Strategie deiner Organisation ab.

Um eine Anwendung im Win32-Format bereitzustellen, wählst du in Intune die Option „**Windows App (Win32)**“ und klickst dann auf „**Select**“. Daraufhin wirst du aufgefordert, eine **App Package File** bereitzustellen.

Diese Datei erstellst du mithilfe des offiziellen Microsoft-Tools **IntuneWinAppUtil.exe**, das auf GitHub zur Verfügung gestellt wird. Du lädst es über den Reiter „**RAW File**“ herunter und speicherst es lokal auf deinem System – empfohlen wird hier ein Ordner wie C:\Temp.



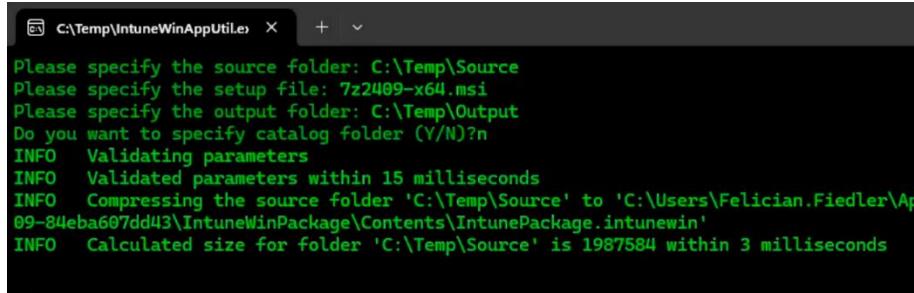
The screenshot shows a GitHub repository page for the Microsoft Win32 Content Prep Tool. At the top, there's a commit by nikyusof-zz fixing an issue with the Win32 content prep tool crashing (#124). Below the commit list, there are links to the README file, Code of conduct, and Security information. The README file itself contains instructions for managing Windows Apps (.intunewin) with Intune and specifies Version 1.8.6.

Bild 164: Content Prep Tool Download

Im nächsten Schritt legst du im Temp-Verzeichnis zwei Unterordner an: „**Source**“ und „**Output**“. In den Source-Ordner kommt die zu paketierende Anwendung. Diese Datei wird heruntergeladen und dann in den Source-Ordner verschoben.

Anschließend startest du die `IntuneWinAppUtil.exe` – das sogenannte **Content Prep Tool**. Das Tool besitzt keine grafische Oberfläche im modernen Sinne, sondern erinnert an ein klassisches Konsolenfenster. Du wirst darin zunächst aufgefordert, den Pfad zum Source-Ordner einzugeben. Danach gibst du den vollständigen Dateinamen der Setup-Datei inklusive Dateiendung ein.

Nach Bestätigung dieser Eingaben beginnt das Tool mit der Konvertierung der MSI-Datei in das Intune-WIN-Format. Die daraus erzeugte Datei wird im Output-Ordner abgelegt und steht anschließend für den Upload in Microsoft Intune zur Verfügung. Dieser Prozess ist die empfohlene Vorgehensweise, um Applikationen im Windows-Umfeld zuverlässig und skalierbar mit Intune zu verteilen.



```
C:\Temp\IntuneWinAppUtil.exe x + v
Please specify the source folder: C:\Temp\Source
Please specify the setup file: 7z2409-x64.msi
Please specify the output folder: C:\Temp\Output
Do you want to specify catalog folder (Y/N)?n
INFO  Validating parameters
INFO  Validated parameters within 15 milliseconds
INFO  Compressing the source folder 'C:\Temp\Source' to 'C:\Users\Felician.Fiedler\AppData\Local\Temp\09-84eba607dd43\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO  Calculated size for folder 'C:\Temp\Source' is 1987584 within 3 milliseconds
```

Bild 165: Umwandlung der Datei

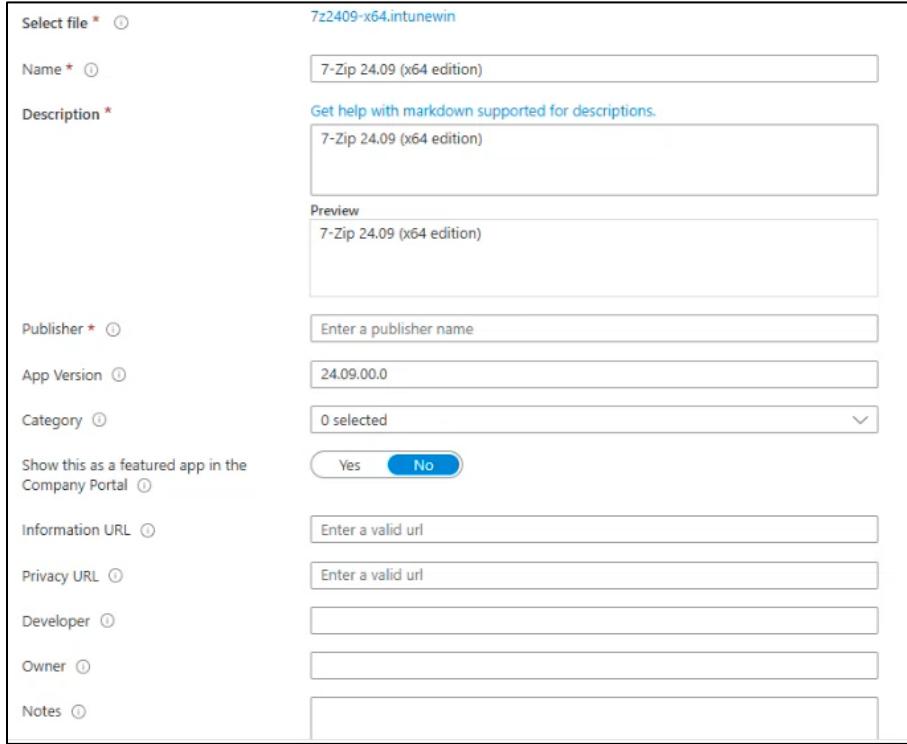
Nachdem du das Content Prep Tool erfolgreich durchlaufen hast, findest du im zuvor definierten **Output-Ordner** deine erzeugte **Intune-WIN-Datei**. Der Grund für die klare Trennung von Source- und Output-Ordner liegt darin, dass der Source-Ordner vollständig sauber und gezielt vorbereitet sein muss. Befinden sich dort zum Beispiel mehrere MSI- oder EXE-Dateien oder zusätzliche Skripte, würde das Tool ein großes, zusammenhängendes Paket daraus schnüren – mit dem Ergebnis, dass die Installation später scheitern könnte. Das Tool erkennt zwar vorhandene Installationsskripte, sortiert sie korrekt ein und verarbeitet sie entsprechend, aber es darf nur das enthalten sein, was wirklich zur Installation notwendig ist. Aus diesem Grund sind zwei getrennte Ordner – „Source“ für Eingaben und „Output“ für das fertige Paket – zwingend erforderlich.

Upload der Intune-WIN-Datei und erste Konfiguration

Nachdem du also deine Intune-WIN-Datei erstellt hast, öffnest du dein **Intune-Portal** und gehst im Bereich **Apps** erneut auf den Punkt „**Select app package file**“, um dort das erzeugte Paket auszuwählen. Es ist wichtig, dass du hier **nicht** die ursprüngliche MSI-Datei auswählst, sondern wirklich das zuvor erstellte **Intune-WIN-Format** verwendest. Obwohl Microsoft die direkte Nutzung von MSI technisch erlaubt, wird sie aus den genannten Gründen explizit nicht empfohlen. Intune liest nach dem Upload der Datei automatisch alle darin enthaltenen Informationen aus. Dazu gehören unter anderem der **Name der Applikation**, eine **Beschreibung** sowie der **Publisher**.

Den Namen der App kannst du an dieser Stelle noch anpassen. In der Regel genügt es, den eigentlichen Produktnamen zu übernehmen und Zusatzinformationen wie Versionsnummern zu

entfernen. Die Beschreibung wird optional angezeigt und kann bei Bedarf noch optisch überarbeitet werden. Der Publisher muss manuell ergänzt werden.



The screenshot shows the 'Edit app' screen in the Microsoft Intune portal. It displays various configuration fields for an application named '7z2409-x64.intunewin'. The fields include:

- Select file: 7z2409-x64.intunewin
- Name: 7-Zip 24.09 (x64 edition)
- Description: Get help with markdown supported for descriptions.
7-Zip 24.09 (x64 edition)
- Preview: 7-Zip 24.09 (x64 edition)
- Publisher: Enter a publisher name
- App Version: 24.09.00.0
- Category: 0 selected
- Show this as a featured app in the Company Portal: No (selected)
- Information URL: Enter a valid url
- Privacy URL: Enter a valid url
- Developer: (empty)
- Owner: (empty)
- Notes: (empty)

Bild 166: Informationen anpassen

Zusätzlich bietet Intune die Möglichkeit, eine **Kategorie** für die Anwendung auszuwählen. Diese Kategorien dienen der **besseren Organisation im Unternehmensportal**, insbesondere bei Apps, die nicht automatisch, sondern optional angeboten werden. Du kannst zwischen vorhandenen Kategorien wählen oder eigene anlegen.

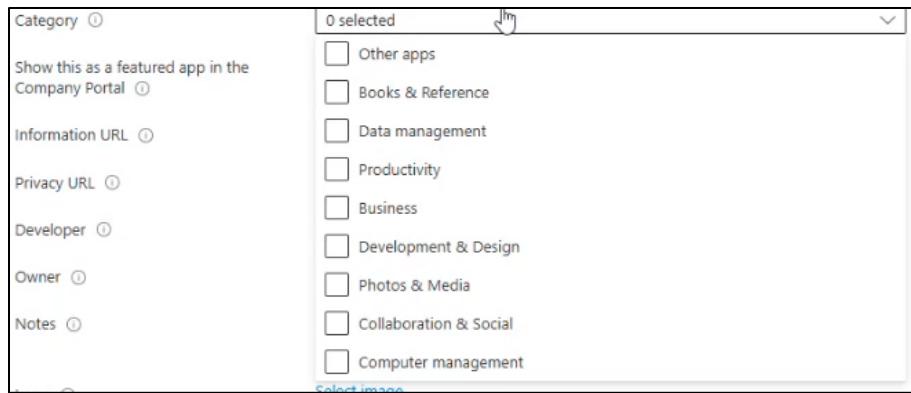


Bild 167: Kategorie

Neue Kategorien erstellst du über die Intune-Oberfläche, indem du auf der linken Seite den Bereich „**Apps**“ auswählst und dann zum Abschnitt „**Organize Apps > App categories**“ navigierst. Dort kannst du über „**Add**“ eine neue Kategorie anlegen, beispielsweise „Data Management“.



Bild 168: App Kategorie erstellen

Zurück im App-Erstellungsprozess kannst du einer dieser Kategorien der App zuweisen. Die restlichen Felder wie **Logo** oder **Select Image** sind optional. Sie werden vor allem dann relevant, wenn die App nicht verpflichtend, sondern optional über das Unternehmensportal bereitgestellt wird – dort kann ein Logo zur besseren optischen Darstellung beitragen. Da in diesem Fall aber eine verpflichtende Installation geplant ist, sind diese Felder nicht notwendig.

Ein optionales Häkchen findest du bei „**Show as a featured app in the Company Portal**“. Wenn diese Option aktiviert ist, wird die App im Unternehmensportal besonders hervorgehoben und in der Übersicht prominent platziert. Auch das ist eher für optionale Bereitstellungen interessant, da erforderliche Anwendungen ohnehin automatisch verteilt werden.

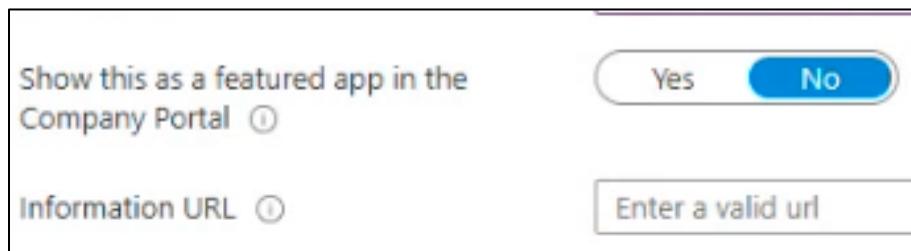


Bild 169: Featured App

Beim Weiterklicken auf „**Next**“ gelangst du in den Abschnitt, in dem Intune versucht, die **Installations- und Deinstallationsparameter** automatisch zu erkennen. Diese Informationen stammen aus der Umwandlung der MSI-Datei in das Intune-WIN-Format. In vielen Fällen gelingt das korrekt, aber es ist nicht garantiert. Wenn die Felder leer bleiben oder fehlerhafte Werte enthalten, musst du diese manuell eintragen.

Zur Ermittlung der korrekten Parameter hast du mehrere Möglichkeiten. Eine gängige Methode ist die Suche über eine Suchmaschine – so, wie es Ivo in einem früheren Beispiel gemacht hat. Ebenso kann ein Blick in die offizielle Dokumentation der Applikation hilfreich sein. Eine besonders praktische Quelle stellt „**Silent Install HQ**“ dar. Diese Website listet zu Tausenden Applikationen die passenden **silent Installationsparameter** auf, inklusive MSI-Befehlen wie `/i`, `/quiet`, `/qn` etc. Du kannst dort gezielt nach dem Programmnamen in Kombination mit „silent install HQ“ suchen, um schnell an die erforderlichen Informationen zu gelangen. Auch wenn es sich hierbei nicht um ein offizielles Microsoft-Tool handelt, ist es dennoch ein häufig genutzter und hilfreicher Dienst.

Im nächsten Schritt findest du das Feld „**Installation time required**“, in dem du angeben kannst, wie viel Zeit die Installation der App typischerweise in Anspruch nimmt. Als Standardwert kannst du beispielsweise 60 Minuten eintragen – dieser Zeitraum sollte in den meisten Fällen mehr als ausreichend sein. Bei Bedarf kannst du diesen Wert natürlich auch anpassen.

Falls die Applikation optional angeboten wird, kannst du zudem festlegen, dass eine **Deinstallation** durch den Nutzer möglich ist. Das geht über die Option „Available uninstall“. Damit gibst du den Anwendern die Freiheit, die Anwendung bei Bedarf auch wieder zu entfernen.

Anschließend wählst du das **Installationsverhalten** über den Parameter „**Install behavior**“ aus. Hier wird zwischen **Systemkontext** und **Userkontext** unterschieden. Intune erkennt in der Regel automatisch, welcher Kontext geeignet ist, wobei standardmäßig der Systemkontext verwendet wird. Das ist in den meisten Fällen auch die richtige Wahl.

Die darunter angezeigten **Rückgabecodes** sind generisch. Es ist wichtig zu wissen, dass **Intune keine eigene Syntax für Installationsbefehle verwendet**. Alles, was du hier einträgst – sei es bei Install- oder Uninstall-Parametern – wird ungeprüft übernommen und erst zur Laufzeit ausgeführt. Intune nimmt also keine Validierung der Befehle vor. Andere MDM-Lösungen verhalten sich hier anders und verlangen teilweise eine spezifische Syntax. Das ist bei Intune jedoch nicht der Fall.

Specify the commands to install and uninstall this app:

Install command *	<input 7z2409-x64.msi\"="" qn"="" type="text" value="msiexec /i \"/>	<input checked="" type="checkbox"/>
Uninstall command *	<input qn"="" type="text" value="msiexec /x \" {23170f69-40c1-2702-2409-000001000000}\"=""/>	<input checked="" type="checkbox"/>
Installation time required (mins) *	<input type="text" value="60"/>	
Allow available uninstall	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Install behavior	<input checked="" type="radio"/> System <input type="radio"/> User	
Device restart behavior	<input type="text" value="App install may force a device restart"/>	

Specify return codes to indicate post-installation behavior:

Return code	Code type	
0	Success	<input type="button" value="Delete"/>
1707	Success	<input type="button" value="Delete"/>
3010	Soft reboot	<input type="button" value="Delete"/>
1641	Hard reboot	<input type="button" value="Delete"/>
1618	Retry	<input type="button" value="Delete"/>

+ Add

Bild 170: Installationsparameter

Wenn du auf „**Next**“ klickst, gelangst du zu den **Requirements**. Intune benötigt hier lediglich zwei Pflichtangaben: die **Betriebssystemarchitektur** und das **Mindestbetriebssystem**. Du klickst also auf „Operating System Architecture“ und wählst dort 64-Bit aus. Anschließend gibst du unter „Minimum Operating System“ die niedrigste unterstützte Version an – zum Beispiel **Windows 11 21H2**, wenn du davon ausgehest, dass eure Clients bereits auf dieser Version laufen. Weitere Felder wie benötigter Speicherplatz, RAM oder logische Prozessoren sind optional und müssen nicht zwingend ausgefüllt werden.

Mit diesen Angaben kannst du anschließend zur nächsten Konfigurationsseite weitergehen – den **Detection Rules**.

Specify the requirements that devices must meet before the app is installed:

Operating system architecture *	64-bit
Minimum operating system *	Windows 11 21H2
Disk space required (MB)	
Physical memory required (MB)	
Minimum number of logical processors required	
Minimum CPU speed required (MHz)	

Configure additional requirement rules

Type	Path/Script
No requirements are specified.	
+ Add	

Bild 171: Requirements

Bei der Konfiguration von **Detection Rules** in Intune ist es entscheidend, eine zuverlässige Methode zu definieren, mit der Intune erkennen kann, ob eine Installation erfolgreich war. Bei MSI-Dateien, die ins Intune-WIN-Format konvertiert wurden, ist der einfachste und zuverlässigste Weg, den **MSI-Produktcode** zu verwenden. Dieser Produktcode wird von Intune automatisch erkannt, wenn man im Setup-Typ „MSI“ auswählt – bei EXE-Dateien hingegen nutzt man den Typ „File“, da hier keine Produkt-ID vorliegt. Intune nutzt, je nach Auswahl, unterschiedliche Mechanismen zur Erfolgskontrolle der Installation. Wenn der MSI-Produktcode korrekt übergeben wurde, erkennt Intune die Installation als erfolgreich. Fehlt diese Detection Rule oder ist sie falsch konfiguriert, führt das zu einem **fehlerhaften Reporting** in Intune – das System könnte dann fälschlich melden, die Installation sei fehlgeschlagen, obwohl sie technisch korrekt durchgeführt wurde. Genauso kann es auch umgekehrt passieren. Daher ist es essenziell, dass diese Erkennungsregel **zu 100 % korrekt** ist.

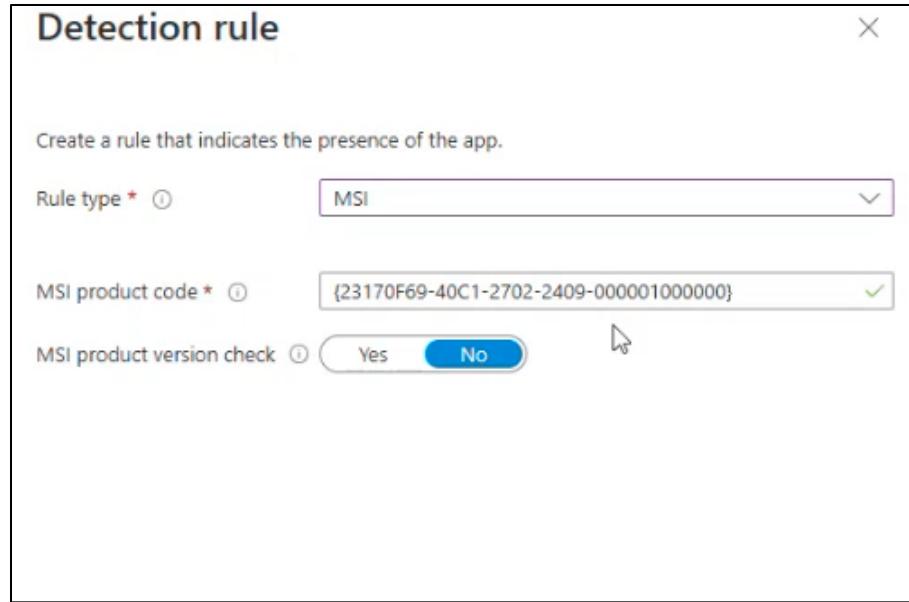


Bild 172: Detection Rules

Nachdem die Detection Rules eingerichtet sind, folgt der Schritt zu den **Dependencies**. Dependencies sind **Abhängigkeiten** zwischen Applikationen. Die Abhängigkeiten können komplex sein – insbesondere in mehrstufigen Installationen wie bei SAP. Dort ist oft eine strikte Reihenfolge einzuhalten, beginnend mit .NET Framework, SQL-Komponenten, Middleware bis hin zum eigentlichen Frontend.

Wenn du in Intune auf „**Add**“ unter Dependencies klickst, kannst du später andere bereits hochgeladene Applikationen als Voraussetzung definieren. Zum Beispiel: Wenn Seven Zip bereits hochgeladen wurde und du nun TeamViewer verteilst, kannst du festlegen, dass TeamViewer nur dann installiert wird, wenn Seven Zip bereits vorhanden ist. Das dient dazu, logische Installationsketten oder **Komponentengruppen** wie Backend → Middleware → Frontend korrekt zu handhaben. Für einfache Tools wie im Beispiel ist das allerdings eher unüblich – der Mechanismus ist vor allem für komplexere Softwarestrukturen gedacht.

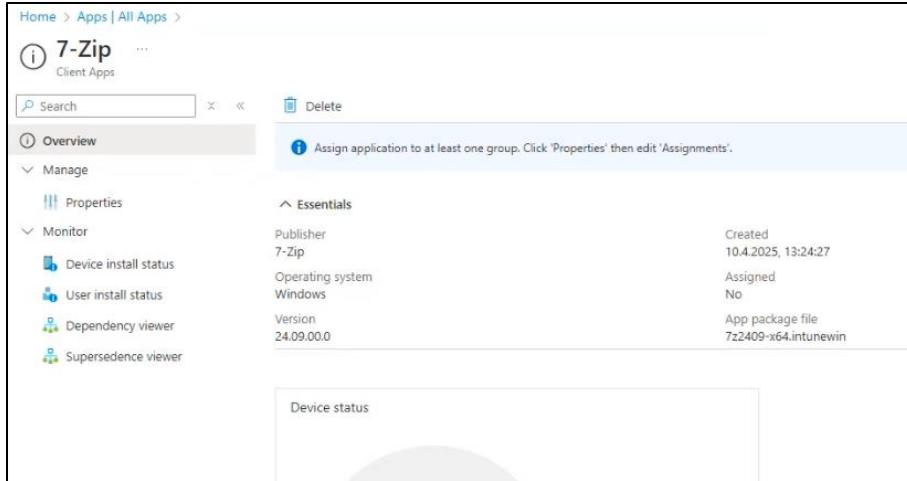
Im Anschluss geht es zum Bereich **Supersedence**. Dieser Mechanismus ermöglicht es, eine bestehende Anwendung durch eine neuere Version zu ersetzen. Du definierst dabei, **welche Applikation (A)** durch eine **neue Applikation (B)** ersetzt werden soll. Das ist der empfohlene Weg, um **Updates über Intune zu verteilen**. Hast du zum Beispiel eine ältere Version von 7-Zip im Einsatz, kannst du beim Hochladen der neuen Version angeben, dass die alte Version

deinstalliert und durch die neue ersetzt werden soll. Damit stellt Supersedence eine zentrale Funktion im Lifecycle Management von Applikationen über Intune dar.

Nach dem Einrichten von Supersedence, also der Möglichkeit, Applikationen durch neuere Versionen zu ersetzen, geht es im nächsten Schritt in Intune zu den **Assignments**. Hier zeigt sich das vertraute Schema mit den drei Zuweisungsarten: „Required“, „Available“ und „Uninstall“. Über „Required“ wird eine App verpflichtend installiert, „Available“ stellt sie optional über das Unternehmensportal bereit, und mit „Uninstall“ kann gezielt eine Deinstallation auf definierten Geräten ausgelöst werden. Eine Anwendung muss also **nicht zwingend direkt installiert werden**, wenn sie hochgeladen wird – sie kann auch nur im Portal verfügbar gemacht oder vorbereitet werden.

Nach der Konfiguration wird der Installationssprozess mit „Create“ abgeschlossen. Kurz darauf erscheint in der Benachrichtigungszentrale oben rechts ein entsprechender Hinweis wie „*Upload of Intune package .intunewin finished*“. Je nach Größe des Pakets kann dieser Vorgang einige Minuten in Anspruch nehmen. Zurzeit gibt es **kein Limit** bei der Anzahl der hochladbaren Applikationen – es sei jedoch denkbar, dass Microsoft künftig ein solches Limit einführt. Dies ist aber derzeit lediglich eine Vermutung.

Mit dieser Aktion wurde nun die erste **MSI-Datei erfolgreich ins Intune-WIN-Format** konvertiert und als Anwendung in Intune bereitgestellt. Diese kann anschließend auf beliebigen Windows-Geräten installiert werden. Der Prozess macht deutlich, dass Intune in Bezug auf Installationsparameter **kein eigenes Framework vorgibt**. Stattdessen hängt die konkrete Konfiguration stark von der jeweiligen Applikation ab – sei es eine MSI oder eine EXE-Datei, jeder Hersteller definiert eigene Parameter, die individuell berücksichtigt werden müssen.



The screenshot shows the Microsoft Intune interface for managing applications. On the left, there's a navigation sidebar with links like 'Home', 'Apps | All Apps', '7-Zip', 'Client Apps', 'Search', 'Delete', 'Overview', 'Manage', 'Properties', 'Monitor', 'Device install status', 'User install status', 'Dependency viewer', and 'Supersedence viewer'. The main content area is titled '7-Zip' and shows the following details:

Essentials	
Publisher	7-Zip
Operating system	Windows
Version	24.09.00.0
Created	10.4.2025, 13:24:27
Assigned	No
App package file	7z2409-x64.intunewin

Below this, there's a section labeled 'Device status'.

Bild 173: Hochgeladene Applikation

Umgang mit individuellen Installationsparametern

In der praktischen Umsetzung vom App Deployment über Microsoft Intune benötigt jede Applikation ihre eigenen spezifischen Parameter für die Installation – ein einheitliches Framework seitens Intune existiert hierbei nicht.

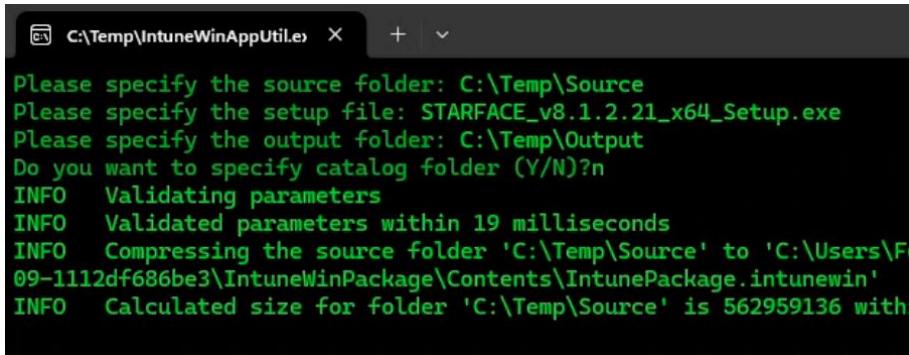
Ein weiteres wichtiges Detail in der Praxis ist die Organisation des *Source*-Ordners. Sammelst du alle Anwendungen in einen gemeinsamen Ordner, führt dies zu gleich großen Ausgabedateien. Die Ursache: Das Pack-Tool nimmt standardmäßig alle Inhalte im Quellverzeichnis auf – unabhängig davon, ob es sich um notwendige oder überflüssige Dateien handelt. Die Lösung hierfür ist, für jede Applikation einen eigenen Unterordner im *Source*-Verzeichnis anzulegen, um gezielt und sauber zu arbeiten.

Grundlagen und Werkzeuge der App-Paketierung in Intune

App-Paketierung ist ein wichtiger, wenn auch oft nicht täglich durchgeführter Bestandteil der Arbeit von IT-Administratoren. Viele Admins sehen sich dabei nicht als klassische App-Paketierer, dennoch ist es wichtig, ein solides Grundverständnis in diesem Bereich zu entwickeln.

– vor allem im Zusammenspiel mit Microsoft Intune. Die Anfangsphase kann mit einer steilen Lernkurve verbunden sein, doch mit zunehmender Routine wird der Prozess deutlich überschaubarer. Besonders essenziell ist hierbei die kontinuierliche Arbeit mit dem *IntuneWinAppUtil*, also dem Content Prep Tool, das zur Erstellung der *.intunewin*-Dateien dient.

Die Anwendung dieses Tools folgt stets einem wiederkehrenden Muster: Es wird der Source-Ordner angegeben, aus dem die Quelldateien stammen, anschließend die ausführbare Installationsdatei (z. B. eine `setup.exe`) definiert, sowie ein Zielordner für die Ausgabe gewählt. Auch wenn das Tool weiterhin Elemente wie den sogenannten *Katalogordner* erzeugt, ist dessen ursprünglicher Zweck – die Unterstützung von Windows 10 S – heute nicht mehr relevant. Der Katalogordner diente früher dazu, IntuneWin-Dateien für das Surface mit Windows 10 S lesbar zu machen. Da dieses System heute keine Rolle mehr spielt, kann dieser Teil vernachlässigt werden.



```
C:\Temp\IntuneWinAppUtil.exe x + ^  
Please specify the source folder: C:\Temp\Source  
Please specify the setup file: STARFACE_v8.1.2.21_x64_Setup.exe  
Please specify the output folder: C:\Temp\Output  
Do you want to specify catalog folder (Y/N)?n  
INFO Validating parameters  
INFO Validated parameters within 19 milliseconds  
INFO Compressing the source folder 'C:\Temp\Source' to 'C:\Users\Fr  
09-1112df686be3\IntuneWinPackage\Contents\IntunePackage.intunewin'  
INFO Calculated size for folder 'C:\Temp\Source' is 562959136 with:
```

Bild 174: Content Prep Tool Exe Datei

Ein weiterer hilfreicher Tipp im Umgang mit ausführbaren Installationsdateien besteht in der Nutzung der PowerShell oder CMD-Konsole. Sollte es Unsicherheiten zu unterstützten Installationsparametern geben (wie z. B. `/silent`, `/verysilent`, `/norestart`), kann man versuchen, durch den Befehl `/?` eine Übersicht über die verfügbaren Parameter aufzurufen. Viele Setupdateien zeigen bei diesem Aufruf eine Hilfeseite oder ein Dialogfenster mit den unterstützten Optionen. Das erleichtert die Ermittlung passender Parameter für die Installation deutlich.

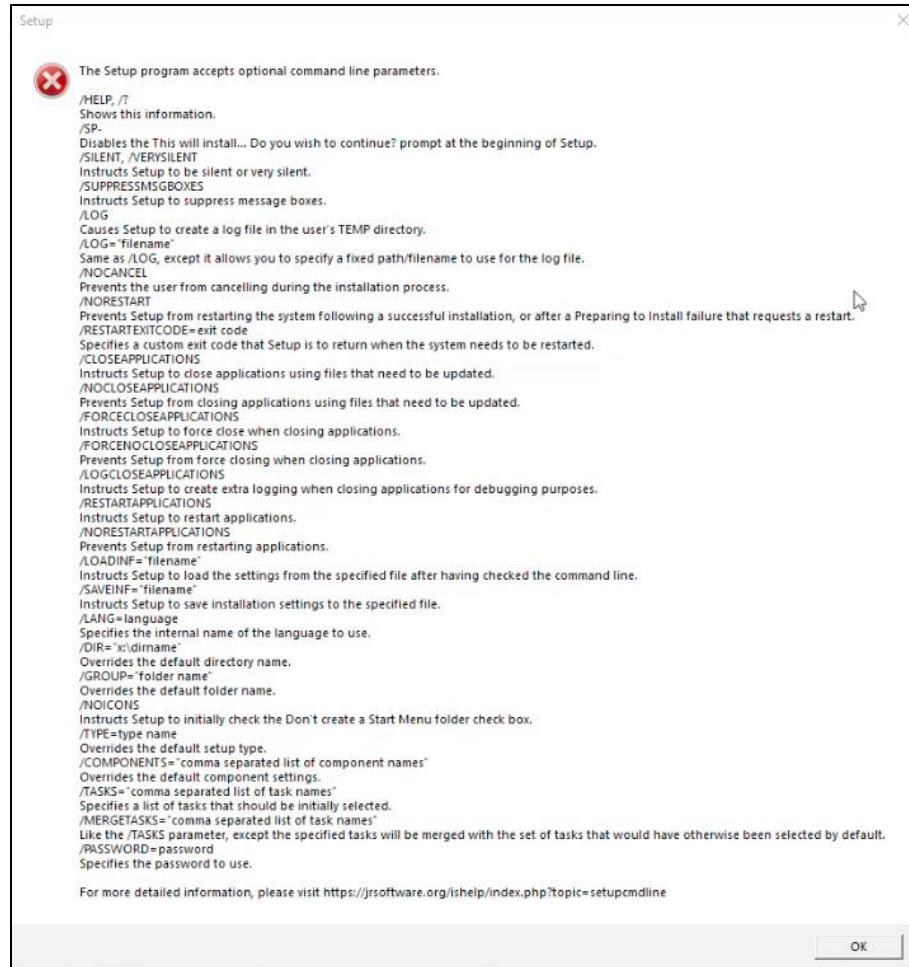


Bild 175: Parameter Applikation

Bei der Paketierung von Anwendungen mit Microsoft Intune spielt die Definition der Installations- und Deinstallationsparameter eine zentrale Rolle. Diese Parameter unterscheiden sich allerdings stark von Anwendung zu Anwendung, da sie vom jeweiligen Softwareanbieter festgelegt werden. Es gibt daher keinen einheitlichen Standard, an den man sich halten kann – weder „/silent“ noch „/qn“ ist universell gültig. Beide Varianten sind gebräuchlich, jedoch muss stets überprüft werden, was vom Entwickler der Anwendung unterstützt wird.

Ein häufiger Fehler betrifft die korrekte Schreibweise von Dateinamen und Pfaden – insbesondere, wenn Leerzeichen enthalten sind. In solchen Fällen müssen die betreffenden Elemente zwingend in Anführungszeichen gesetzt werden. Beispiel:

"Starface Installer.exe" /silent

Hierbei ist es wichtig, konsistent zu arbeiten: Wird der Pfad oder der Dateiname in Anführungszeichen gesetzt, sollte auch geprüft werden, ob weitere Parameter korrekt übergeben werden und keine Syntaxfehler entstehen. Auch dies hängt teilweise von der Anwendung selbst ab – manche Programme benötigen Anführungszeichen, andere akzeptieren den Pfad auch ohne.

Im praktischen Umgang empfiehlt es sich, den Namen der Anwendung in Intune möglichst klar und nachvollziehbar zu benennen. Zusätze wie die Version (z. B. „Starface (V8–21)“) helfen dabei, die Übersicht in der App-Liste zu behalten. Optional können auch Beschreibungen ergänzt oder angepasst werden – etwa durch Herausfiltern unnötiger Informationen oder durch Einfügen zusätzlicher Hinweise zur Versionierung.

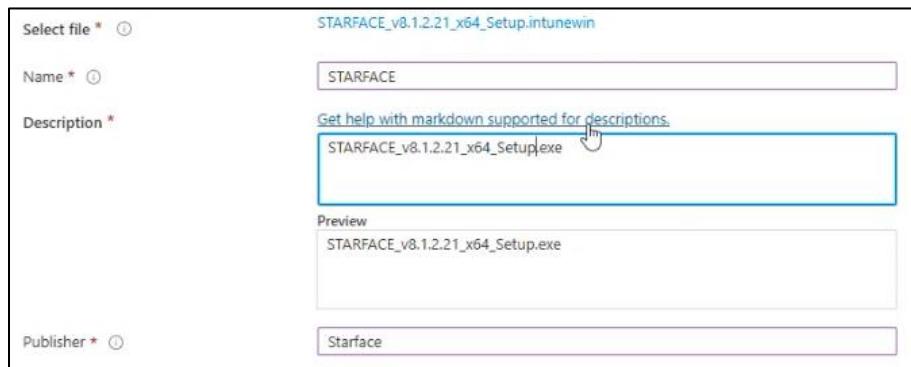


Bild 176: Beschreibung mit Version

Ein App-Icon oder ein Bild (unter „Logo“) kann zwar hochgeladen werden, ist für die Funktion der Verteilung jedoch nicht notwendig. Es kann – vor allem in Testumgebungen oder bei internen Tools – bewusst ausgelassen werden.

Ein weiterer wichtiger Punkt ist die korrekte Handhabung von Pfaden in den Befehlen. Wenn im Installations- oder Uninstallationsbefehl ein Pfad mit Leerzeichen enthält (z. B. C:\Program Files\...), muss dieser Pfad zwingend in Anführungszeichen gesetzt werden. Andernfalls interpretiert die Kommandozeile nur den ersten Teil bis zum Leerzeichen und bricht den Befehl mit einem Fehler ab. Wird jedoch lediglich der Name der ausführbaren

Datei verwendet – ohne vollständigen Pfad – sind Anführungszeichen nur dann erforderlich, wenn auch der Dateiname selbst Leerzeichen enthält.

Ob ein vollständiger Pfad notwendig ist, ergibt sich ebenfalls aus der Dokumentation des Herstellers. Wird dort nur die ausführbare Datei genannt (z. B. `setup.exe`), kann auf einen vollständigen Pfad verzichtet werden. Gibt der Hersteller hingegen einen festen Pfad an (z. B. `%ProgramFiles%\Hersteller\Anwendung\uninstall.exe`), muss dieser auch exakt so angegeben werden – insbesondere, wenn er Teil des Uninstall-Befehls ist.

Bei weiteren Einstellungen wie der maximalen Installationsdauer (Installation time) empfiehlt es sich, einen realistischen Pufferwert zu wählen – etwa 60 Minuten für größere Anwendungen. Der Installationsmodus sollte in der Regel auf „System“ gesetzt werden, da so die Installation systemweit erfolgt und nicht benutzergebunden ist. Auch ein durch die Installation ausgelöster Neustart sollte – je nach Art der Anwendung – zugelassen werden, insbesondere bei verpflichtenden Deployments. Bei optionalen Anwendungen hingegen kann ein Neustart unterdrückt werden, um Nutzerunterbrechungen zu vermeiden.

Die Konfiguration der Rückgabecodes (Return codes) kann meist unverändert übernommen werden, da Intune hier bereits sinnvolle Standardwerte hinterlegt. Diese Standardwerte decken gängige Erfolgscodes und Fehlerfälle ab, ohne dass zusätzlicher Anpassungsbedarf besteht.

Insgesamt gilt: Die Eingaben in Intune richten sich nicht nach einer festen Struktur innerhalb von Intune selbst, sondern müssen stets entlang der technischen Vorgaben des Herstellers erfolgen. Eine saubere und korrekte Umsetzung dieser Vorgaben ist entscheidend für eine fehlerfreie Installation und Deinstallation über Intune.

Specify the commands to install and uninstall this app:

Install command *	STARFACE_v8.1.0.12_x64_Setup.exe /silent	✓
Uninstall command *	"C:\Program Files\STARFACE\unins000.exe" /silent	✓
Installation time required (mins)	60	
Allow available uninstall	Yes <input checked="" type="radio"/> No <input type="radio"/>	
Install behavior	System <input checked="" type="radio"/> User <input type="radio"/>	
Device restart behavior	App install may force a device restart	

Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

Bild 177: Program App

Bei der Definition der Detection Rules innerhalb von Microsoft Intune ist es entscheidend, die tatsächlichen Gegebenheiten auf dem Zielsystem zu berücksichtigen. Da moderne Systeme in der Regel auf 64-Bit-Architekturen basieren und häufig bereits mit Windows 11 betrieben werden, reichen diese Angaben im Normalfall für die grundlegenden Installationsanforderungen aus. Komplexer wird es jedoch, wenn es darum geht, die tatsächliche Existenz einer Anwendung auf einem Gerät nachzuweisen – also die sogenannten Detection Rules korrekt zu konfigurieren.

Specify the requirements that devices must meet before the app is installed:

Operating system architecture *	64-bit	▼
Minimum operating system *	Windows 11 21H2	▼
Disk space required (MB)		
Physical memory required (MB)		
Minimum number of logical processors required		
Minimum CPU speed required (MHz)		
Configure additional requirement rules		
Type	Path/Script	
No requirements are specified.		

Bild 178: Requirements

Wenn keine automatische Erkennung wie bei MSI-Dateien möglich ist, wird empfohlen, manuelle Detection Rules zu definieren. In solchen Fällen sollte nicht etwa der temporäre Output-Ordner verwendet werden, in dem sich die gepackte .intunewin-Datei befindet, sondern es ist wichtig, den tatsächlichen Installationspfad der Anwendung auf dem Clientgerät zu prüfen. Entscheidend ist, dass der Pfad auf eine Datei oder einen Ordner verweist, der nach der erfolgreichen Installation sicher vorhanden ist – typischerweise die .exe-Datei der Anwendung im Installationsverzeichnis.

Die Erkennungsmethode kann dabei variieren. Ein gängiger und sehr universeller Ansatz ist die Methode „**File or folder exists**“. Diese ist besonders geeignet, wenn keine spezifische Herstellerdokumentation vorliegt oder keine speziellen Registrierungswerte oder Versionsstrings geprüft werden müssen. Liegt jedoch eine klare Vorgabe des Herstellers vor – wie etwa bei bestimmten Microsoft-Tools, die einen Registry-String oder eine bestimmte Dateiversion zur Verifikation empfehlen – dann sollte diese auch genutzt werden. Die Wahl der Methode hängt also vom jeweiligen Fall ab: „File or folder exists“ ist breit einsetzbar, während „String comparison“ oder „Version check“ dann sinnvoll sind, wenn präzise Bedingungen oder Werte bekannt sind.

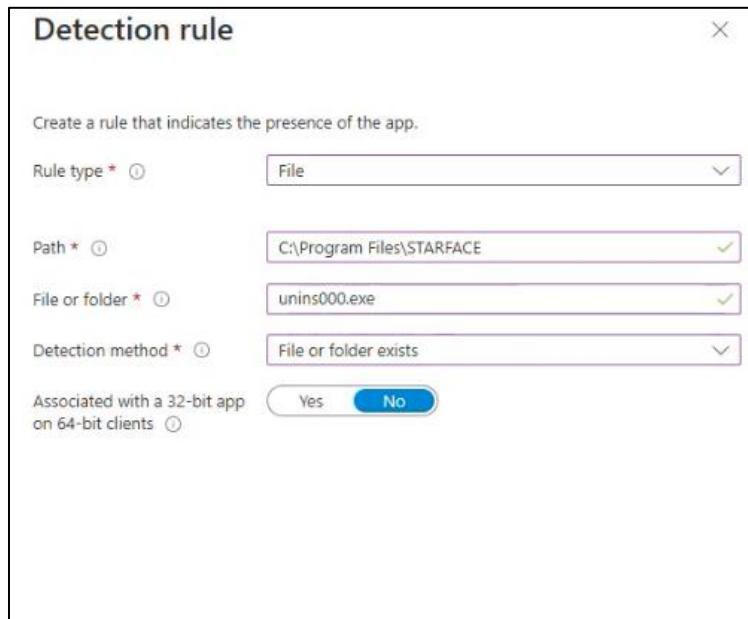


Bild 179: Detection rules

Für die Konfiguration von Anwendungen in Intune genügt in der Regel eine einzige Detection Rule, sofern sie korrekt gesetzt ist. Weitere Regeln können ergänzt werden, sind aber meist nicht notwendig. Bei der Paketierung sollten auch die **Dependencies** berücksichtigt werden – also Abhängigkeiten zu anderen Anwendungen, die vorab installiert sein müssen. Beispielsweise könnte eine Anwendung wie 7-Zip als Voraussetzung definiert werden, bevor eine weitere App installiert wird.



Bild 180: Dependencies

Ebenso lassen sich im Abschnitt **Supersedence** Vorgängerversionen definieren, die durch das neue Paket ersetzt oder deinstalliert werden sollen. Wird beispielsweise eine ältere Version erkannt, kann diese gezielt entfernt werden, um einen sauberen Zustand sicherzustellen.

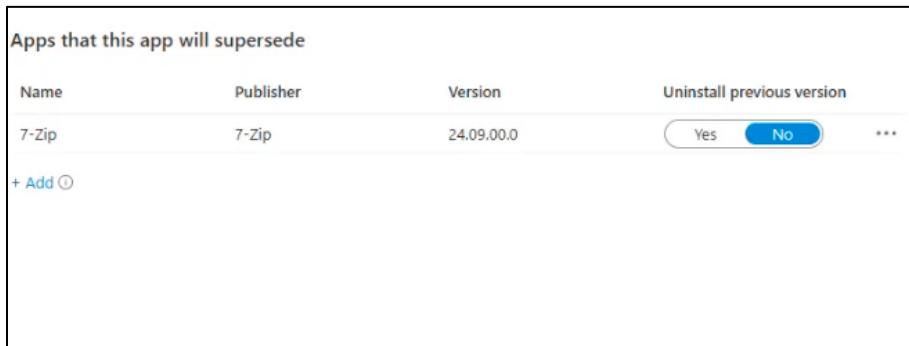


Bild 181: Supersedence

Beim Erstellen des Pakets kann es vereinzelt zu Upload-Fehlern kommen, etwa wenn die Dateiübertragung im Hintergrund unterbrochen wird. In solchen Fällen hilft es, das Paket

einfach erneut auszuwählen und hochzuladen – ein Anwenderfehler liegt in solchen Situationen in der Regel nicht vor.

Das zugrunde liegende Schema zur App-Bereitstellung in Intune ist grundsätzlich wiederverwendbar: Anwendungen – ob `.msi` oder `.exe` – werden stets ins **Intune-Win-Format** überführt. Zu Beginn kann dieser Prozess komplex wirken, da viele Variablen zu berücksichtigen sind. Mit zunehmender Routine wird die Struktur jedoch klarer und lässt sich vergleichsweise effizient auf weitere Applikationen übertragen. Wer bereits mit anderen Softwareverteilungslösungen wie Baramundi gearbeitet hat, wird feststellen, dass Intune mehr technische Tiefe erfordert und dadurch nicht ganz so intuitiv wirkt. Dennoch bietet es eine hohe Flexibilität, gerade im Zusammenspiel mit modernen Gerätekonfigurationen.

Bei der Zuweisung von Applikationen empfiehlt Microsoft die Nutzung von **Gerätegruppen**, da so eine konsistenter und stabilere Zuweisung möglich ist. In bestimmten Szenarien – etwa bei Mitarbeitern, die an mehreren Geräten arbeiten – kann alternativ mit **Benutzergruppen** gearbeitet werden, wenn eine App personenbezogen bereitgestellt werden soll.

Darüber hinaus lassen sich im Rahmen der App-Paketierung auch zusätzliche ausführbare Dateien integrieren, etwa **.cmd-, .bat-, .dll- oder .ps1-Skripte**. Das verwendete Content Prep Tool erkennt diese Dateien zuverlässig und bindet sie korrekt ein. Dadurch lässt sich die Verteilung auch komplexerer Setups realisieren, ohne auf externe Hilfsmittel angewiesen zu sein.

Einige Anwendungen, wie etwa Gaza oder der UBQ Manager, bringen ihre eigenen Abhängigkeiten wie Microsoft Visual C++ oder die Desktop Runtime bereits mit und installieren diese automatisch. Das kann im Vergleich zu anderen Anwendungen hilfreich sein, bei denen solche Komponenten manuell berücksichtigt und eingebunden werden müssen.

Tools, Dienste und Alternativen zur manuellen Paketierung

Für die Bereitstellung von Anwendungen über Intune gibt es neben der manuellen Paketierung auch unterstützende Tools und Dienste, die diesen Prozess erheblich vereinfachen. Während man mit Bordmitteln und etwas mehr Zeit sämtliche Installationspakete selbst erstellt und konfiguriert, bieten Drittanbieter bereits vorgefertigte Pakete an oder übernehmen die gesamte Paketierung. Zwei bekannte Beispiele hierfür sind **Chocolatey** und **Scappman**. Beide Tools dienen als App-Paketierungsplattformen, mit denen sich Softwareinstallationen zentral verwalten und automatisch bereitstellen lassen. Sie bieten Zugriff auf große App-Bibliotheken mit mehreren tausend Anwendungen und übernehmen sowohl die Bereitstellung als auch das Patch-Management.

Besonders positiv hervorgehoben wurde Scappman, da es bei vergleichsweise geringen Kosten eine solide Leistung bietet – zum Beispiel rund 1.200 € jährlich für etwa 450 Endgeräte. Auch **Patch My PC** ist in diesem Zusammenhang ein geläufiger und weit verbreiteter Anbieter, der in vielen Unternehmen zum Einsatz kommt. Solche Tools lassen sich gut in bestehende Intune-Strukturen integrieren und helfen, Zeit und Aufwand zu sparen.

Wer lieber auf kostenfreie Varianten setzen möchte, kann auf Lösungen wie den **Win Tuner** zurückgreifen. Dabei handelt es sich um ein PowerShell-basiertes Tool, das den Paketierungsvorgang vereinfacht. Statt zahlreiche Einzelbefehle manuell abzusetzen, lassen sich hier mit nur wenigen Zeilen Code vollständige App-Pakete erzeugen. Auch hierzu existieren bereits hilfreiche Tutorials und Videos – etwa auf YouTube von „Get Rubix“ – die Schritt für Schritt zeigen, wie man mit dem Tool arbeiten kann.

Kapitel 33: Reporting und Auswertung in Intune – Richtlinien, Compliance und Log-Analyse

Zunächst findest du im linken Navigationsbereich unter dem Punkt "**Reports**" verschiedene Berichtsfunktionen. Diese ermöglichen dir die Analyse von Log-Dateien und Konfigurationsdaten.

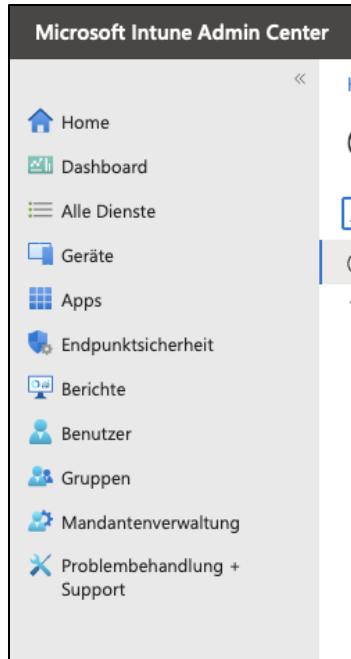


Bild 182: Reports

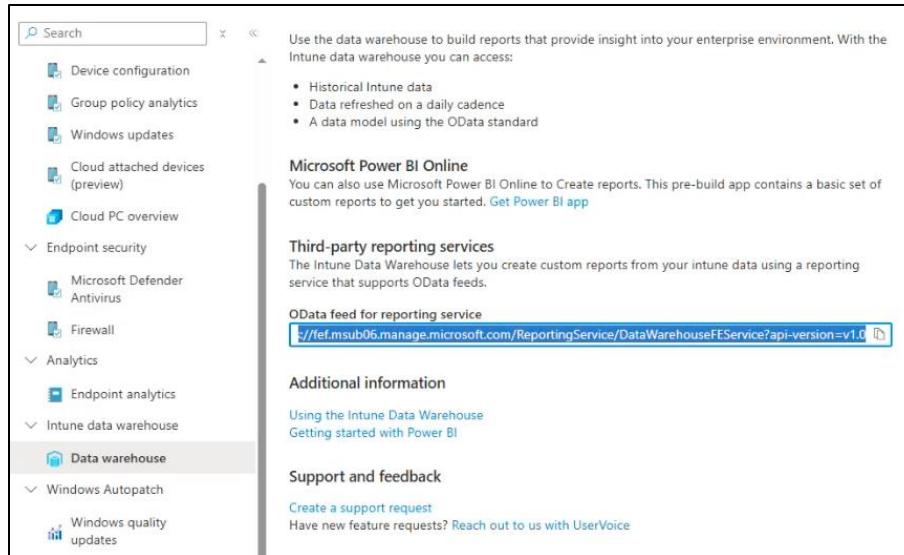
Unter "**Device Configuration**" kannst du beispielsweise den "**General Report**" einsehen, der dir einen Überblick über den Zustand deiner Richtlinien liefert. Weiter unten findest du unter "**Policy Configuration Status**" detailliertere Berichte, bei denen du über verschiedene Filter – etwa das Betriebssystem oder den Richtlinientyp – Reports generieren kannst. Diese zeigen dir, welche Richtlinien wie häufig fehlschlagen oder wo Fehler auftreten. Dabei handelt es sich um eine Übersicht, die dir eine fundierte Bewertung darüber ermöglicht, ob Konfigurationen korrekt angewendet wurden oder ob es an bestimmten Stellen zu Problemen kommt. Es ist möglich, die angezeigten Spalten (Columns) im Report individuell anzupassen, um die Darstellung deinen Anforderungen anzupassen. So kannst du gezielt herausfiltern, welche Konfigurationsrichtlinien oder Applikationen an welchen Geräten fehlschlagen oder Auffälligkeiten zeigen.

Policy name	Policy type	OS	Successful devices
Allow Microsoft App Store Updates	Settings Catalog	Windows10	264
Antivirus-Win10	Microsoft Defender Antivirus	Windows10	278
Block ChatGPT	Custom	MacOS	59
Block-Cloudapps	Settings Catalog	MacOS	59
Defender for Endpoint	Microsoft Defender for Endpoint (desktop...)	Windows10	282

Bild 183: Policy Configuration Status

Diese Reports stehen nicht nur für die Konfigurationsrichtlinien zur Verfügung, sondern auch für "**Device Compliance**". Dort kannst du einsehen, welche Geräte nicht konform sind und auf Basis welcher Einstellungen oder Konfigurationen diese Abweichung auftritt. Die Reports dienen also als zusätzliches Analysewerkzeug für deine IT-Infrastruktur.

Falls du jedoch außerhalb von Intune detailliertere Analysen benötigst, bietet dir Microsoft über den Punkt "**Intune Data Warehouse**" eine erweiterte Möglichkeit. Dort findest du einen sogenannten **Datafeed**, der sich gezielt an Nutzer richtet, die mit Visualisierungstools wie **Power BI** arbeiten. Über diesen Datafeed kannst du dir eigene Dashboards in Power BI aufbauen, die sich etwa alle acht Stunden automatisch aktualisieren. Auf diesem Weg lassen sich tiefergehende Auswertungen und Visualisierungen realisieren. Die Erstellung solcher Dashboards erfordert jedoch Kenntnisse im Bereich Power BI und Datenmodellierung. Falls du dich mit Power BI bislang nicht intensiv auseinandergesetzt hast, wirst du eventuell etwas Einarbeitungszeit benötigen, kannst dir aber so ein leistungsfähiges Analysewerkzeug schaffen.



The screenshot shows the Microsoft Intune Data Warehouse page. On the left, there's a navigation sidebar with a search bar at the top. Below it are several categories: Device configuration, Group policy analytics, Windows updates, Cloud attached devices (preview), Cloud PC overview, Endpoint security (with Microsoft Defender Antivirus and Firewall), Analytics (with Endpoint analytics), Intune data warehouse (which is expanded to show Data warehouse), Windows Autopatch, and Windows quality updates. The 'Data warehouse' section is highlighted with a yellow box. To the right of the sidebar, there's a main content area. At the top, it says 'Use the data warehouse to build reports that provide insight into your enterprise environment. With the Intune data warehouse you can access:'. Below this is a bulleted list: 'Historical Intune data', 'Data refreshed on a daily cadence', and 'A data model using the OData standard'. Underneath is a section titled 'Microsoft Power BI Online' with a sub-section 'Third-party reporting services'. It mentions the Intune Data Warehouse lets you create custom reports from your intune data using a reporting service that supports OData feeds. A blue box highlights the 'OData feed for reporting service' URL: <https://lef.msub06.manage.microsoft.com/ReportingService/DataWarehouseFEService?api-version=v1.0>. Below this are sections for 'Additional information' (links to 'Using the Intune Data Warehouse' and 'Getting started with Power BI'), 'Support and feedback' (link to 'Create a support request'), and 'Have new feature requests? Reach out to us with UserVoice'.

Bild 184: Data Warehouse

Eine zusätzliche Möglichkeit zur Erweiterung der Reporting-Funktionalitäten bieten sogenannte **Workbooks**. Beachte jedoch, dass diese Workbooks **nicht Bestandteil deiner Microsoft 365-Umgebung** sind. Sie gehören ausschließlich zu einer **Azure-Subscription** und erfordern entsprechende Berechtigungen sowie eine aktive Azure-Umgebung. Sie stehen dir also nur dann zur Verfügung, wenn dein Unternehmen auch über eine Azure Subscription verfügt und diese für Intune-Zwecke nutzt.

Darüber hinaus kannst du auch über den Menüpunkt "**Devices**" weitere Analysen vornehmen. Wenn du in diesem Bereich den Unterpunkt "**Monitor**" auswählst, erhältst du Zugriff auf zusätzliche Reports. Dazu gehören beispielsweise Informationen zum "**Device Encryption Status**", also dem aktuellen Verschlüsselungsstatus der verwalteten Geräte. Hiermit kannst du unter anderem nachvollziehen, welche Geräte bereits durch BitLocker abgesichert sind und welche noch nicht. Solche Informationen können für deine Sicherheitsrichtlinien von entscheidender Bedeutung sein.

Device name	OS	OS version	TPM version	Encryption readiness	Encryption status
ALEX_XEMPIUS	Windows	10.0.26100.3476	2.0	Ready	Encrypted
AlexandrovWaldemar	Windows	10.0.22631.4890	2.0	Ready	Encrypted
B-NBWP-22687	Windows	10.0.19045.5600	2.0	Ready	Encrypted
BAZAVALERIIA	Windows	10.0.22631.3737	2.0	Ready	Encrypted
BIEHLOVAALBINA	Windows	10.0.22631.3737	2.0	Ready	Encrypted
BUNETSKAOLENA	Windows	10.0.22631.3737	2.0	Ready	Encrypted

Bild 185: Device Encryption

In Intune lässt sich nicht nur der Status installierter Applikationen überwachen, sondern auch deren Verwaltung zentral durchführen. Unter dem Menüpunkt *Monitor* kann eingesehen werden, welche Anwendungen auf welchen Geräten installiert sind und in welchem Zustand sich die Installation befindet. Darüber hinaus besteht die Möglichkeit, einzelne Anwendungen gezielt zu deinstallieren. Eine spezielle Funktion stellt der sogenannte *App Selective Wipe* dar, mit dem sich gezielt nur die unternehmenseigenen Applikationen von einem Gerät entfernen lassen, ohne das gesamte Gerät zurückzusetzen. Diese Funktion ist jedoch ausschließlich auf iOS- und Android-Geräten verfügbar und steht für Windows-Geräte nicht zur Verfügung.

Im Bereich *Tenant Administration* lässt sich unter dem Punkt *End User Experiences > Customization* die Darstellung des Unternehmensportals anpassen. Hier können unter anderem das Unternehmenslogo sowie die Farbschemata definiert werden, sodass das Portal optisch zur Corporate Identity passt. Standardmäßig ist die Darstellung in Blau gehalten, kann aber an die eigene Farbwelt angepasst werden. Neben dem visuellen Branding lassen sich auch Kontaktinformationen und andere unternehmensspezifische Hinweise hinterlegen, die den Endbenutzern im Unternehmensportal angezeigt werden. So entsteht ein professioneller, wiedererkennbarer Auftritt, der zusätzliches Vertrauen bei den Mitarbeitenden schafft und zur Orientierung beiträgt.

Branding	
Name der Organisation	siller.consulting
Designfarbe	#007233
In Kopfzeile anzeigen	Nur Organisationsname
Supportinformationen	
Kontaktname	Aaron Siller
Telefonnummer	015736589796
E-Mail-Adresse	aaron@siller.consulting
Websitename	siller.consulting
Website-URL	http://www.siller.consulting
Zusätzliche Informationen	Keine Zusätzliche Informationen
Konfiguration	
Geräteregistrierung	Verfügbar, mit Eingabeaufforderungen
URL zur Datenschutzerklärung	http://www.siller.consulting
Datenschutzmeldung zu den für den Support nicht sichtbaren Elementen und zu den vom Support nicht durchführbaren Aktionen (iOS/iPadOS)	Standard
Inhalt eingeben	Keine Inhalt eingeben
Datenschutzmeldung zu den für den Support sichtbaren Elementen und zu den vom Support durchführbaren Aktionen (iOS/iPadOS)	Standard

Bild 186: End User Experience

Im Bereich *Connectors and Tokens* innerhalb von Intune lassen sich verschiedene externe Dienste und Partnerlösungen anbinden, um die Funktionalität rund um Gerätemanagement und Sicherheitsbewertung zu erweitern. Ein typisches Beispiel ist die Integration von Apple VPP (Volume Purchase Program), das die zentrale Verwaltung von iOS-Anwendungen ermöglicht. Darüber hinaus stehen unter den *Cross Platform Settings* diverse Optionen zur Verfügung, um Konnektoren zu Drittanbieter-Lösungen für mobile Sicherheitsplattformen zu integrieren.

Diese Schnittstellen ermöglichen es, ergänzende Sicherheitsinformationen – etwa von Anbietern wie Trend Micro, Check Point, Symantec oder Zimperium – in die Intune-Verwaltung zu überführen. Besonders sinnvoll kann dies sein, wenn nicht ausschließlich auf Microsoft Defender for Endpoint gesetzt werden soll. Stattdessen lassen sich über diese Integrationen externe Sicherheitslösungen einbinden, deren Bewertungen und Bedrohungsanalysen in das eigene Compliance- und Gerätemanagement einfließen können.

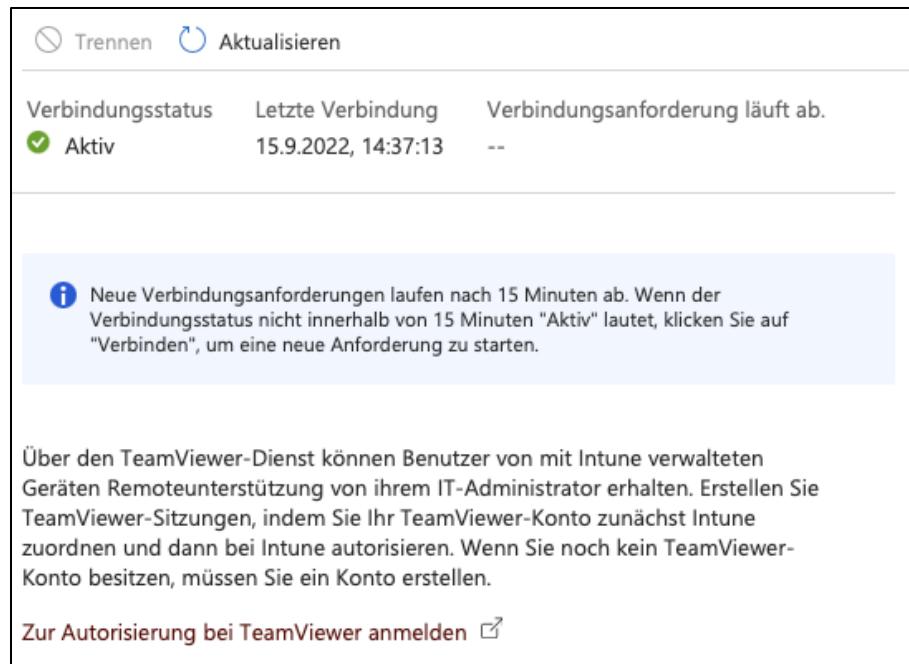
Darüber hinaus existieren spezielle Partnerprogramme wie *Mobile Threat Defense* oder *Partner Compliance Management*. Über diese lassen sich auch Geräte einbinden, die primär durch andere Mobile Device Management (MDM)-Lösungen verwaltet werden – zum Beispiel mit

Maas360, MobileIron, Workspace ONE oder anderen weniger bekannten MDM-Plattformen. Für diese Geräte kann die Compliance-Bewertung in Intune übernommen und mit Conditional Access verknüpft werden. So lässt sich sicherstellen, dass nur konforme Geräte Zugriff auf Unternehmensressourcen erhalten, auch wenn diese nicht nativ in Intune registriert sind. Dies eröffnet flexible Einsatzmöglichkeiten in heterogenen IT-Umgebungen, in denen verschiedene MDM-Tools im Einsatz sind.

Nutze die verschiedenen Berichte und Monitoring-Funktionen in Intune, um den Status deiner Geräteflotte, Konfigurationen und Anwendungen jederzeit im Blick zu behalten. Dabei helfen dir sowohl die integrierten Reporting-Werkzeuge in Intune als auch erweiterte Lösungen wie Power BI oder Azure Workbooks, um eine fundierte und transparente Übersicht über deine IT-Umgebung zu schaffen.

Kapitel 34: Remote-Support, Audit-Logs und Group Policy Analytics in Intune

Für den Remote-Support über Intune besteht die Möglichkeit, TeamViewer zu nutzen. Von der direkten Integration des TeamViewer-Connectors in Intune ist jedoch abzuraten. Der Connector dient primär dazu, eine Verbindung zwischen Intune und TeamViewer herzustellen, wobei eine Authentifizierung im TeamViewer Admin Center erforderlich ist. Nach Einrichtung kann über Intune eine Remoteunterstützungssitzung angestoßen werden. Dabei öffnet sich TeamViewer jedoch nicht automatisch beim Endanwender. Stattdessen muss der Nutzer manuell in die Unternehmensportal-App wechseln, dort auf ein entsprechendes Symbol klicken und den Prozess von dort aus starten. Diese zusätzliche Interaktion sorgt für eine unnötige Zwischenschicht, die den Supportprozess nicht effizienter macht. Die generelle Nutzung von TeamViewer oder vergleichbaren Lösungen als Support-Tool ist weiterhin möglich und sinnvoll – lediglich die direkte Intune-Integration bringt an dieser Stelle keinen praktischen Vorteil.



The screenshot shows the TeamViewer Connector interface. At the top, there are two buttons: "Trennen" (Disconnect) with a crossed-out lock icon and "Aktualisieren" (Update) with a circular arrow icon. Below this, there is a table with three columns:

Verbindungsstatus	Letzte Verbindung	Verbindungsanforderung läuft ab.
✓ Aktiv	15.9.2022, 14:37:13	--

Below the table, a blue information box contains the following text:

i Neue Verbindungsanforderungen laufen nach 15 Minuten ab. Wenn der Verbindungsstatus nicht innerhalb von 15 Minuten "Aktiv" lautet, klicken Sie auf "Verbinden", um eine neue Anforderung zu starten.

At the bottom of the interface, there is a note: "Über den TeamViewer-Dienst können Benutzer von mit Intune verwalteten Geräten Remoteunterstützung von ihrem IT-Administrator erhalten. Erstellen Sie TeamViewer-Sitzungen, indem Sie Ihr TeamViewer-Konto zunächst Intune zuordnen und dann bei Intune autorisieren. Wenn Sie noch kein TeamViewer-Konto besitzen, müssen Sie ein Konto erstellen." followed by a link "Zur Autorisierung bei TeamViewer anmelden" with a small icon.

Bild 187: TeamViewer-Connector

Neben dieser Variante steht auch die Microsoft Remotehilfe zur Verfügung. Diese lässt sich in Intune integrieren und funktioniert in der Praxis zuverlässig. Sie wird beispielsweise von manchen Unternehmen als primäres Supportwerkzeug genutzt. Es ist jedoch zu beachten, dass die Integration in Intune kostenpflichtig ist – obwohl das Tool selbst grundsätzlich kostenlos zur Verfügung steht. Für den produktiven Einsatz im Supportkontext sollte dieser Aspekt mit einkalkuliert werden.

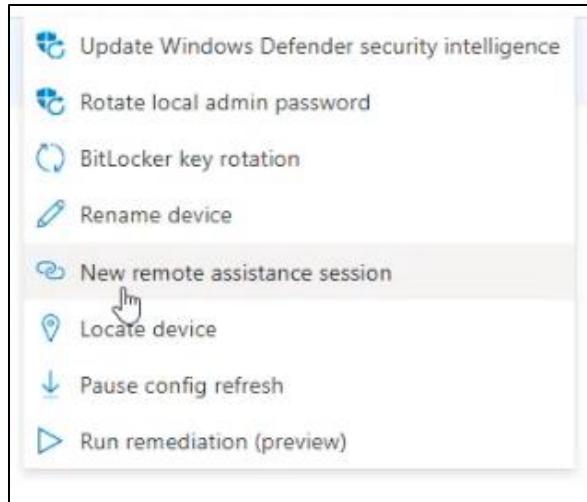


Bild 188: Microsoft Remotehilfe

Ein weiteres wichtiges Werkzeug innerhalb von Intune sind die Audit Logs. Sie dienen der Nachvollziehbarkeit administrativer Aktivitäten innerhalb der Umgebung. Erfasst werden dabei unter anderem das Erstellen von Clients, Änderungen an Zertifikaten, Löschvorgänge von Benutzerkonten oder das Zurücksetzen von Geräten. Diese Informationen sind essenziell für die Überwachung und Protokollierung von Konfigurations- und Managementvorgängen in administrativen Umgebungen.

Date ↓	Initiated by (ac...)	Application na...	Activity
04/10/2025, 12:...			Create ClientCe...
04/10/2025, 12:...	engin.avcilar@...		Create ClientCe...
04/10/2025, 12:...			Create ClientCe...
04/10/2025, 11:...	enginadm@xe...	Microsoft Intu...	Delete Manage...
04/10/2025, 11:...			Create ClientCe...
04/10/2025, 11:...			Create ClientCe...

Bild 189: Audit Logs

Ergänzend dazu bieten die „Diagnostic Settings“ die Möglichkeit, weiterführende Logs – wie etwa Operationslogs oder DeviceCompliance-Informationen – zu erfassen und an eine Azure Subscription weiterzuleiten. Diese Funktion eröffnet erweiterte Analyseoptionen über Azure-

Tools und sollte dort eingesetzt werden, wo detaillierte Auswertungen und langfristige Protokollierung erforderlich sind.

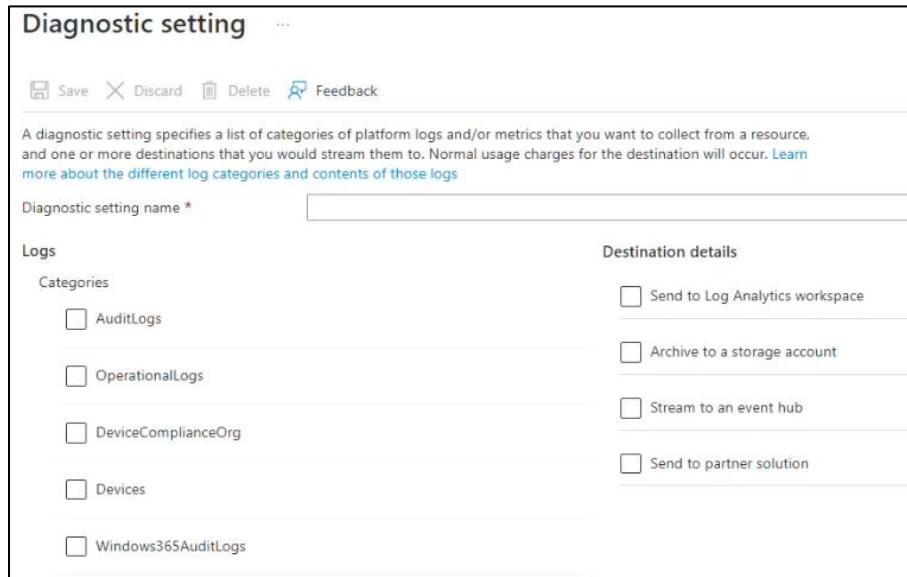


Bild 190: Diagnostic Settings

Die Rubrik „Help and Support“ innerhalb Intune ermöglicht es, bei technischen Problemen direkt Supportanfragen an Microsoft zu stellen. Über „Microsoft Support“ oder den kontextbezogenen Support-Bereich lassen sich Themen direkt adressieren. Die Qualität des Supports ist dabei variabel. Ein konstant hochwertiger Support ist nur über dedizierte Premium-Support-Modelle zu erwarten, welche nicht im Microsoft-365- oder Intune-Abonnement enthalten sind und separat kostenpflichtig gebucht werden müssen.

Ein weiteres nützliches Tool im Troubleshooting-Kontext ist die Benutzer-basierte Fehleranalyse. Über das Menü „Troubleshooting + Support“ lassen sich für einzelne Benutzer – inklusive deren zugeordneter Geräte – gezielt Probleme und Fehlermeldungen einsehen. Auch die Gruppenzugehörigkeit und Richtlinienzuweisungen werden hier angezeigt. Diese Übersicht eignet sich besonders zur Analyse von Policy-Zuweisungsproblemen und Compliance-Verstößen.

			Refresh	Export	Columns
Name ↑	Targeting	Assignment			
WinGet-AutoUpdate-Configurator	User	Included			
Allow Microsoft App Store Updates	User	Included			
Block ChatGPT	User	Included			
Block-Cloudapps	User	Included			
Compliance-Policy-MacOS	User	Included			

Bild 191: Troubleshoot

Im Bereich der Richtlinienverwaltung bietet Intune mit den „Group Policy Analytics“ eine Möglichkeit, bestehende Gruppenrichtlinien aus Active Directory zu analysieren. Die Funktion erlaubt das Hochladen von ADMX-Dateien, um zu prüfen, inwieweit diese sich mit integrierten MDM-Konfigurationsrichtlinien abbilden lassen. Die Analyse basiert auf einem CSP-Mapping (Configuration Service Provider), das häufig etwa 50 % der klassischen Gruppenrichtlinieneinstellungen mit nativen Intune-Mitteln als umsetzbar einstuft. Dennoch bietet es sich in vielen Fällen an, die ADMX-Vorlagen direkt hochzuladen, um vollständige Kompatibilität und Flexibilität zu gewährleisten.

Setting name ↑↓	Group policy setting category ↑↓	MDM support ↑↓
Always automatically restart at the schedul...	Windows Components/Windows Update	⚠ No
Automatic Updates detection frequency/in...	Windows Components/Windows Update	✓ Yes
Configure Automatic Updates/Configure a...	Windows Components/Windows Update	✓ Yes
Configure Automatic Updates/Install durin...	Windows Components/Windows Update	✓ Yes
Configure Automatic Updates/Install updat...	Windows Components/Windows Update	⚠ No

Bild 192: Group Policy Analytics

Weitere Funktionen wie das Umbenennen von Geräten („Rename Device“), das Zurücksetzen lokaler Administratorpasswörter („Rotate local admin password“), Updates der Windows Defender Security Intelligence oder der direkte Zugriff auf Geräteeinstellungen über Intune runden die Werkzeuge zur Geräteverwaltung ab. Diese Optionen ermöglichen es, auch ohne zusätzliche Tools direkt aus Intune heraus zentrale administrative Aufgaben durchzuführen.

Beim Thema Paketierung von Anwendungen im Kontext von Intune stehen verschiedene Lösungen zur Auswahl, abhängig davon, ob und wie viel Budget für externe Tools zur Verfügung steht. Eine besonders einfache und kostenfreie Option stellt **Win Tuner** dar. Obwohl weniger bekannt, bietet diese Lösung eine erhebliche Vereinfachung des Paketierungsprozesses, indem sie aus zahlreichen Einzelschritten nur wenige macht. Wer keine externen Dienstleister beauftragen möchte, kann mit Win Tuner effizient arbeiten und dennoch einen strukturierten Deployment-Prozess aufbauen – vorausgesetzt, man ist bereit, die Pakete selbst zu erstellen.

Für eine vollständig automatisierte Lösung, bei der weder Paketierung noch regelmäßige Updates selbst durchgeführt werden müssen, empfiehlt sich **Patch My PC**. Dabei handelt es sich um einen Dienstleister, der den vollständigen Lifecycle von Anwendungen übernimmt – von der Bereitstellung über die Aktualisierung bis hin zur Verwaltung. Unternehmen können über eine zentrale Plattform Anwendungen anfragen, die dann paketiert und direkt über Intune bereitgestellt werden. Diese Lösung richtet sich vor allem an IT-Umgebungen, in denen möglichst wenig manuelle Arbeit beim Applikationsmanagement gewünscht ist. Wichtig zu wissen ist, dass Patch My PC in der Regel kostenpflichtig ist und nur eingeschränkt Testversionen anbietet.

Weitere Alternativen wie **Scappman** oder **Chocolatey** bieten ähnliche Ansätze. Chocolatey stellt eine besonders einsteigerfreundliche Testumgebung bereit, während Scappman ursprünglich als Empfehlung galt, bis kritische Hinweise in der Praxis auftraten. Der **Enterprise App Manager** oder das **Enterprise App Management** von Microsoft ist ebenfalls zu nennen, da es sich hierbei um eine native Lösung innerhalb des Microsoft-Ökosystems handelt. Diese Option erfordert allerdings meist eine gesonderte Lizenzierung.

Letztlich hängt die Wahl der passenden Lösung stark von den Anforderungen und Ressourcen ab: Wer möglichst wenig selbst machen möchte, greift zu einem Dienstleister wie Patch My PC. Wer hingegen kosteneffizient und flexibel bleiben will, kann mit Tools wie Win Tuner oder direkt über Intune eigenständig Paketierung und Verteilung umsetzen.

Schlusswort: Dein Weg zu einer sicheren Microsoft 365 Umgebung

Mit den Inhalten dieses E-Books verfügst du nun über das notwendige Wissen, um deine Microsoft 365 Umgebung sowie Microsoft Entra ID strukturiert und praxisorientiert abzusichern. Angefangen bei der Verwaltung von Benutzerkonten und Gruppen bis hin zu detaillierten Gerätekonfigurationen in Intune sowie dem gezielten Einsatz von Conditional Access und App Protection Policies – jede einzelne Maßnahme leistet ihren Beitrag zur Reduktion von Risiken und zur Steigerung der Betriebssicherheit.

Wichtig ist jedoch: Die Arbeit endet nicht mit der Umsetzung der beschriebenen Maßnahmen. Microsoft 365 und Entra ID sind dynamische Plattformen. Neue Funktionen, geänderte Lizenzmodelle oder sich wandelnde Bedrohungslagen erfordern eine kontinuierliche Anpassung deiner Konfiguration.

Beachte daher folgende Grundprinzipien für den laufenden Betrieb:

- **Kontinuität:** Überprüfe regelmäßig bestehende Sicherheitsrichtlinien und Konfigurationen. Passe diese an aktuelle technische und organisatorische Anforderungen an.
- **Automatisierung:** Setze auf Werkzeuge wie Microsoft Intune, Defender for Endpoint oder Entra ID Governance, um manuelle Fehlerquellen zu minimieren und Prozesse effizient zu gestalten.
- **Awareness:** Sorge für ein einheitliches Sicherheitsverständnis im Unternehmen durch verbindliche Richtlinien und regelmäßige Schulungen der Mitarbeitenden.

Sicherheit ist kein statischer Zustand, sondern ein fortlaufender Prozess. Die in diesem Leitfaden vermittelten technischen Grundlagen bieten dir eine verlässliche Ausgangsbasis, um deine Microsoft 365 Umgebung zielgerichtet zu betreiben, weiterzuentwickeln und zukunftssicher aufzustellen.

Empfehlung für die Praxis: Beginne mit den Bereichen, die das höchste Risikopotenzial oder die größte Reichweite haben. Setze dann nach und nach weitere Maßnahmen um. So erhöhst du

sukzessive den Sicherheitsstandard und die Stabilität deiner Umgebung – mit einem klar strukturierten, kontrollierten Vorgehen.