WINDOWS DEVICES - 1 - INTUNE ERSTINSTALLATION

Vorarlberger Standardschulinstallation
Verfasser: Dietmar Köb, Lukas Franz, Kuno Sandholzer, Martin Schnetzer

> ⚠ Diese Anleitung wurde im Jahr 2021 erstellt und ist in einigen Bereichen nicht mehr vollständig aktuell. Die grundlegenden Inhalte bleiben jedoch weiterhin gültig. Bei Fragen oder Unklarheiten verweisen wir auf die aktuelle Dokumentation zur Serverlosen Schule.

1 Grundsätzliches

1.1 Voraussetzungen:

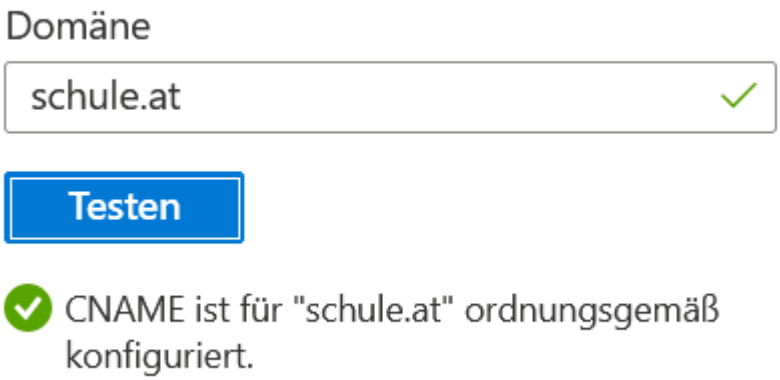
- Tenant der Schule ist fertig eingerichtet
- Administratorzugang zu MS-365 ist vorhanden
- CNAME – EnterpriseEnrollment und EnterpriseRegistration kontrollieren

Admin-Center: Einstellungen - Domänen - “meineschule.at” - DNS-Einträge (https://admin.microsoft.com)

Basic-Mobilität und Sicherheit

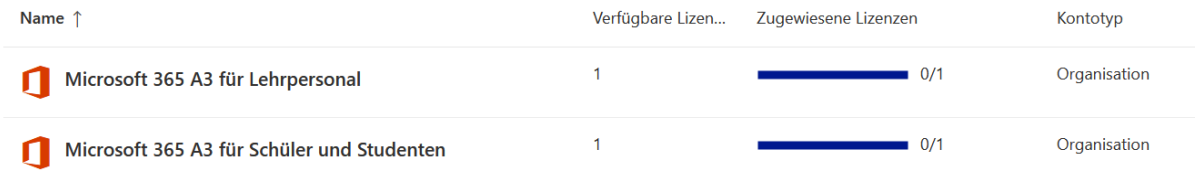
Typ	Status	Name	Wert
CNAME	OK	enterpriseregistration	enterpriseregistration.windows.net
CNAME	OK	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com

Endpoint: Geräte - Geräte registrieren – Windows-Registrierung – CNAME-Validierung



- A3-Lizenzen sind dem Tenant zugeordnet und der Menüpunkt „Endpoint Manager“ oder „Endpunkt-Manager“ ist im „Microsoft 365 admin center“ vorhanden

Admin-Center: Abrechnung – Lizenzen



Admin-Center: Alle Admin Center

WLAN:

- temporäres WLAN (mit einfachem Passwort) für die “Rollout” Stunden (für die erste(n) Unterrichtsstunden “Digitale Grundbildung” mit den neuen Geräten)
- Daten für das produktive WLAN für die neuen Geräte (SSID + Passwort)

1.2 Konzept:

Einsatz von Autopilot:

Vom Lieferanten bekommen wir bei den Windows-Tablets die Seriennummern und die dazu passenden Hardware-Hashes. Mit diesen beiden Werten kann die für den Autopilot-Import notwendige “csv-Datei” befüllt werden.

Hinweis: Die “Microsoft Product Key ID” steht auf dem Karton drauf, ist aber für den csv-Import nicht notwendig bzw. nützt da auch nicht wirklich etwas. Sie ist aber eine Alternative, wenn der Hardwarehash nicht zur Verfügung steht, wie das bei den Windows-Notebooks von Lenovo der Fall ist. Dann muss die Autopilot-Registrierung aber von einem autorisierten Händler (z.B. ACP – Felix Huber kennt sich aus) gemacht werden: In diesem Fall werden die Geräte direkt über ein Online-Portal registriert und nach einem Synchronisierungsvorgang in Intune (Windows AutoPilot-Geräte) werden die Laptops aufgelistet.

Windows-Tablets:
Die Registrierung der Geräte erfolgt über einen CSV-Import. Diese csv-Datei enthält diese Felder:

- Device Serial Number (Plicht – bekommen wir vom Lieferanten)
- Windows Product ID (für den Import über eine CSV-Datei nicht erforderlich)
- Hardware Hash (Plicht – bekommen wir vom Lieferanten)
- Group Tag: N21LuL, N20SuS, …
- Assigned User: Wird bei den Schülergeräten und Lehrergeräten verwendet. Damit ist auch vorab der Benutzer in Intune als Besitzer des Gerätes hinterlegt.

Optionen für die Lehrergeräte:

Option 1:
Das Lehrergerät ist einer bestimmen Lehrperson zugeordnet. Wird diese Option gewählt, so wird die betreffende Lehrperson in das Feld Assigned User eingetragen. Diese ist Besitzer und Administrator des Geräts.

Option 2:
Das Lehrergerät ist ein Poolgerät, welches von mehreren LehrerInnen verwendet wird. Wird diese Option gewählt, so wird ein „Dummy-User“, welcher Besitzer des Geräts ist, in das Feld Assigned User eingetragen (z.B.: lehrergeraet@schule.at + A1-Lizenz). Es kann für alle diese Poolgeräte der gleiche “Dummy-Account” verwendet werden.

⚠ Es werden dadurch zwei unterschiedliche Bereitstellungsprofile erstellt, welche sich nur in einem Punkt unterscheiden: Bei “Option 1” bekommt der Benutzer, der sich als erster am Gerät anmeldet, lokale Administratorrechte, bei “Option 2” nicht (siehe Kap. 4.3).

Dynamische Zuordnung zu den entsprechenden Gerätegruppen

Über den jeweiligen Group Tag (Synonyme an anderen „Stellen“: Order ID; Gruppentag) in der CSV-Datei werden die Geräte automatisch den entsprechenden Gerätegruppen („Minimalversion“: N21LuL; N20SuS; N21SuS) zugeordnet („N“ für Notebooks – „T“ für Tablets; „20“ (6. Klassen) bzw. „21“ (5. Klassen) für das Eintrittsjahr). Dafür werden dynamische Gerätegruppen verwendet.

Für jeden Gruppentag (also dann auch für jede Gerätegruppe) muss ein eigenes Autopilot-Profil erstellt werden, in welchem dann auch der Gerätename definiert wird – z.B.:

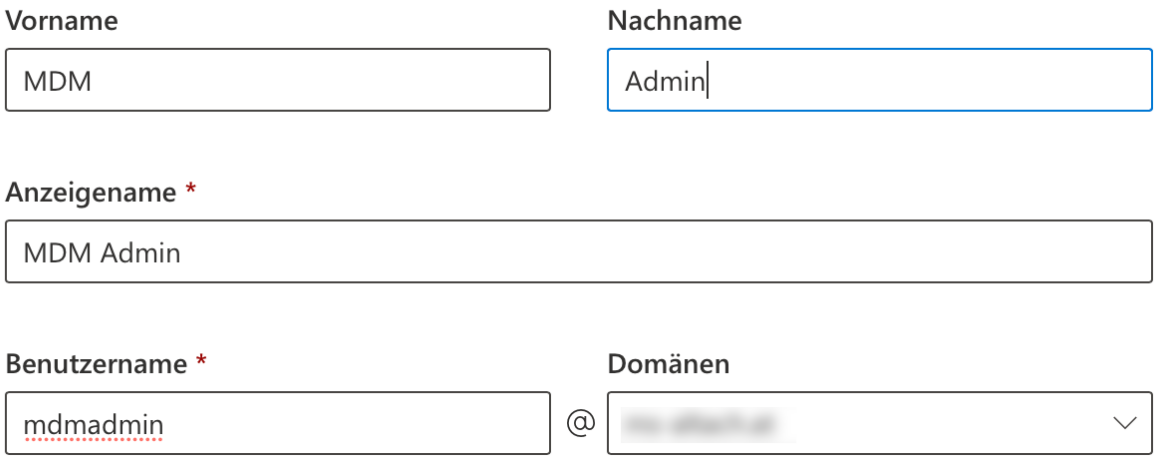
- 21L-%SERIAL% (neue Lehrergeräte, die im Herbst 21 registriert wurden)
- 20S-%SERIAL% (neue Schülergeräte von SuS, die im Herbst 20 in der 5. Klasse waren, also im SJ 21/22 die „6. Klässler”)
- 21S-%SERIAL% (neue Schülergeräte von SuS der 5. Klassen (= im Herbst 2021))

ⓘ Der Gerätename darf nur max. 15 Zeichen lang sein. Viele Seriennummern sind 10 Zeichen lang (deshalb vor der Seriennummer nur 4 oder 5 Zeichen). Ist die Seriennummer zu lang, wird sie beim Erstellen des Gerätenamens abgeschnitten (oftmals aber leider nicht von hinten, sondern von vorne – dann fehlen also die ersten Zeichen der Seriennummern im Gerätenamen und das ist lästig)!

1.2.1 Eigener Administrator für das Mobile Device Management

Falls die Verwaltung der Apps und Geräte von einer anderen Person als dem IT-Betreuer gemacht wird, so kann ein eigener Administrator nur für den Endpoint Manager erstellt werden.

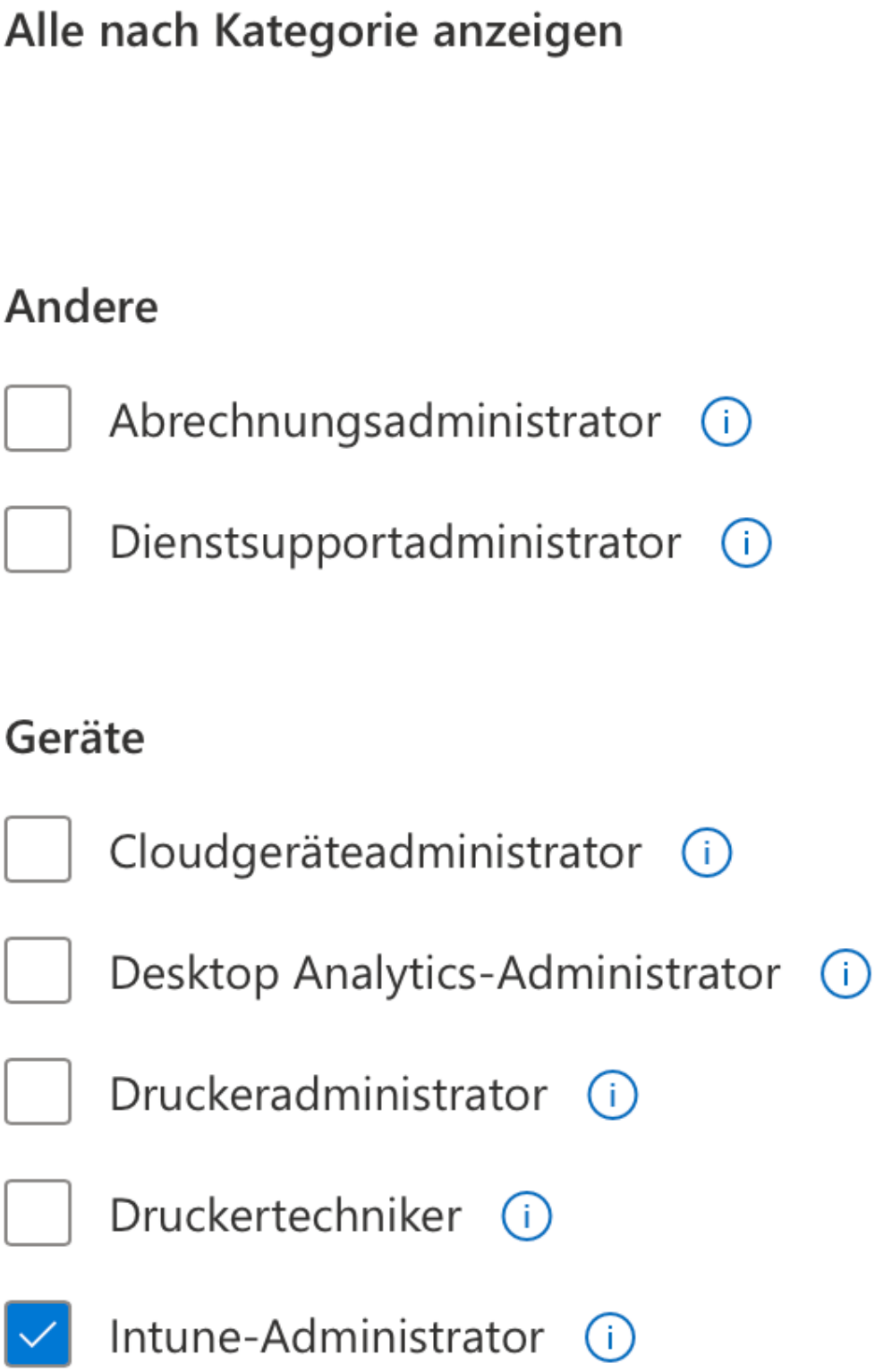
“Microsoft 365 admin center”: Benutzer – Aktive Benutzer – Benutzer hinzufügen



Als Lizenz reicht eine einfache „Office 365 A1-Lizenz für Lehrpersonal“.

Bei den Rollen „Admin Center-Zugriff“ auswählen und anschließend „Alle nach Kategorie anzeigen“ anklicken, damit alle Administrator-Optionen angezeigt

werden. Im Bereich „Geräte“ findet sich der „Intune-Administrator“.



Mit diesem Zugang kann nun direkt auf https://intune.microsoft.com zugegriffen werden.

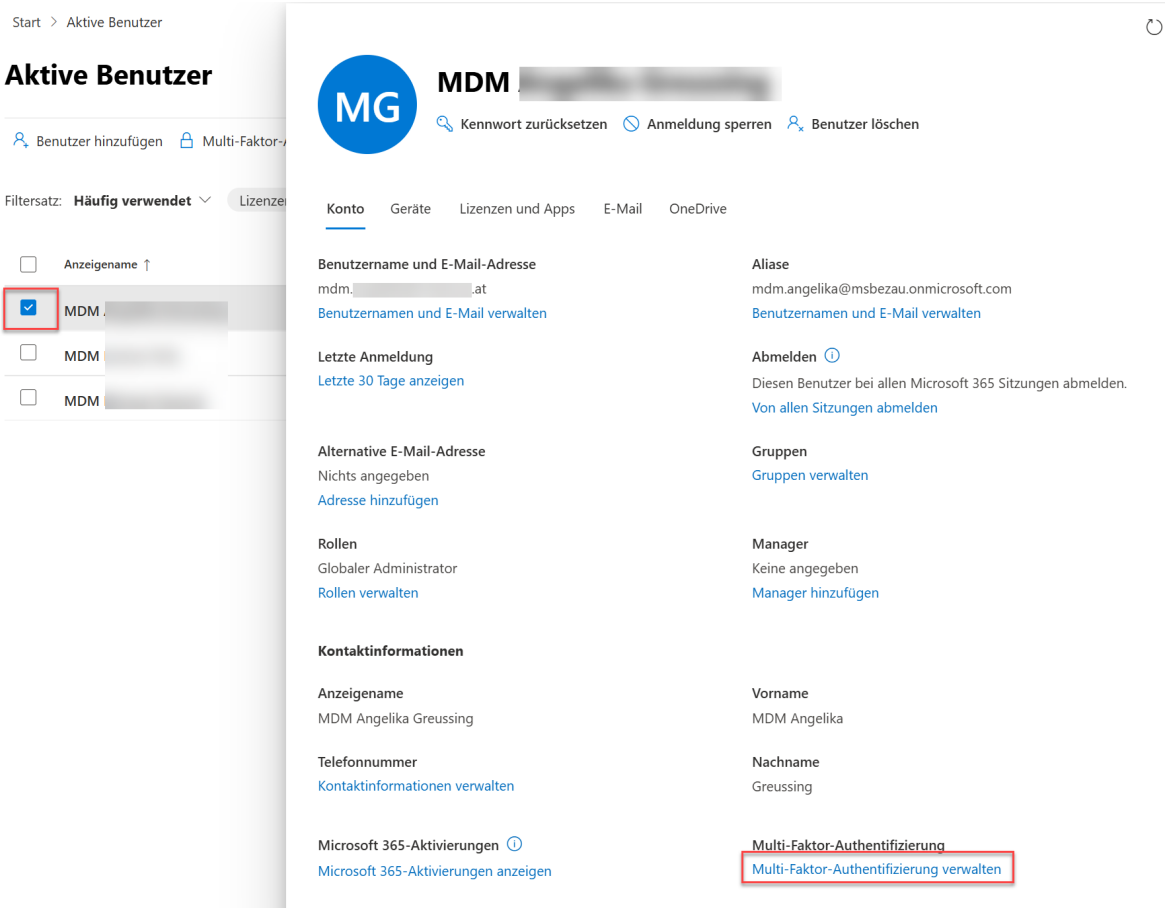
1.2.2 Mehrstufige Authentifizierung

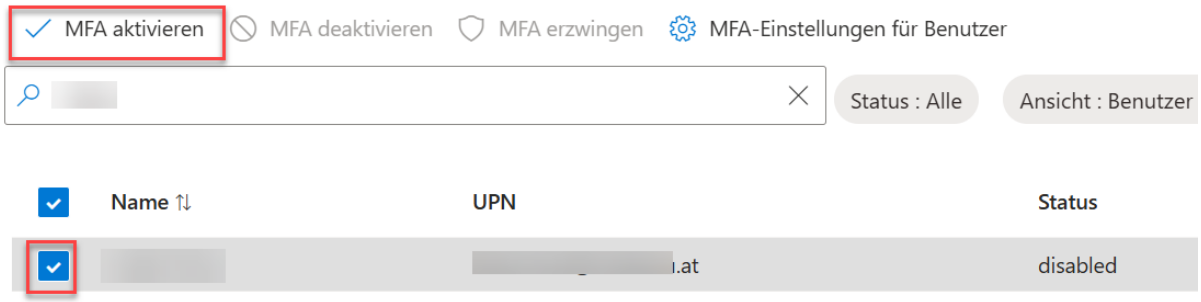
1.2.2.1 Allgemeines

> ⚠ Die missbräuchliche Verwendung des Administratorenkontos birgt sehr große Sicherheitsgefahren. Dadurch ist es erforderlich, Konten der Administratorengruppe mit der mehrstufigen Authentifizierung abzusichern.

1.2.2.2 Konfiguration

- Öffne das Admin Centers (https://admin.microsoft.com)
- Aktive Benutzer > einen Benutzer öffnen
- Mehrstufige Authentifizierung verwalten klicken
- Administrator Benutzer auswählen > aktivieren
- Informationen zum Aktivieren bestätigen



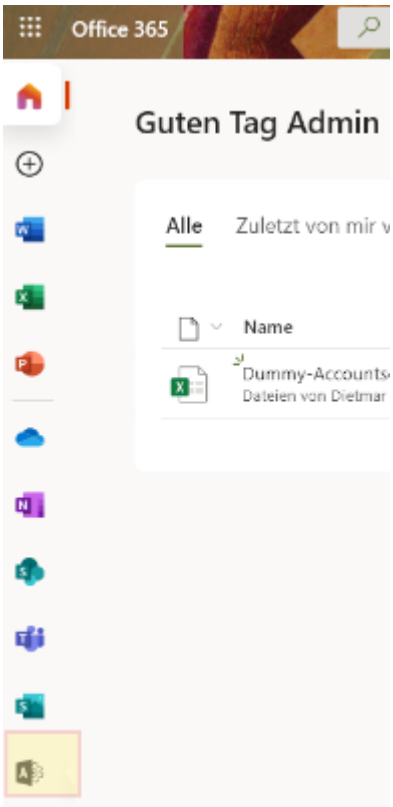


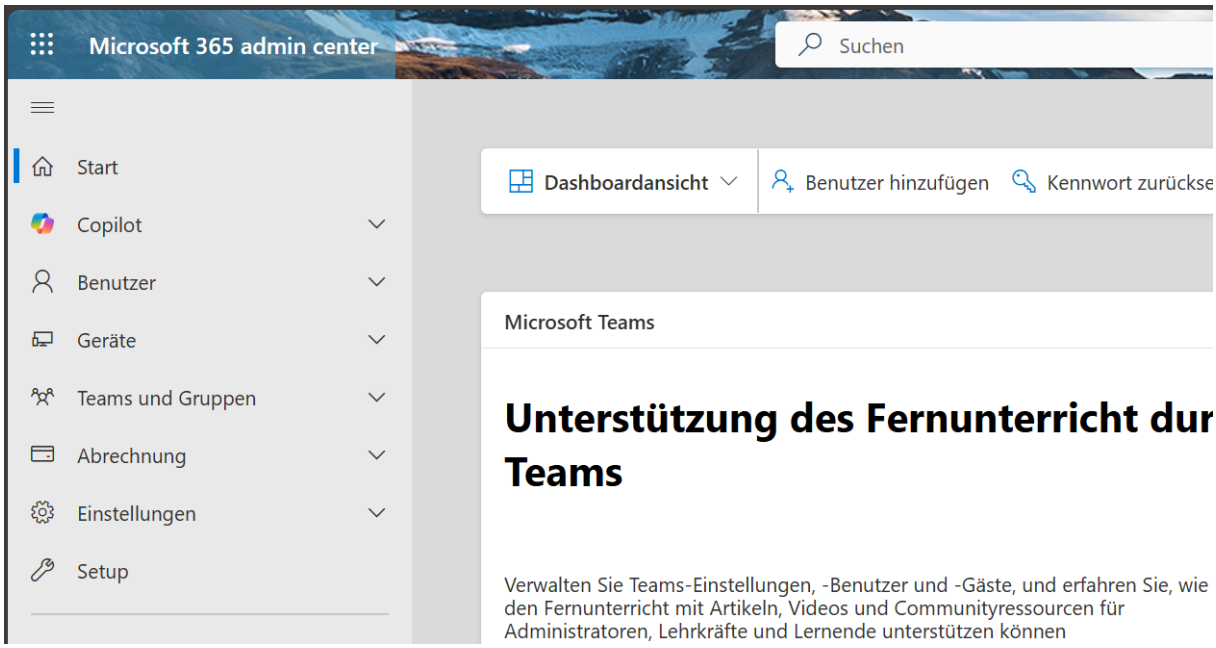
2 Die verschiedenen Plattformen

2.1 Die allgemeine MS-365-Verwaltungsoberfläche:

https://m365.cloud.microsoft

Login als MS365-Administrator:

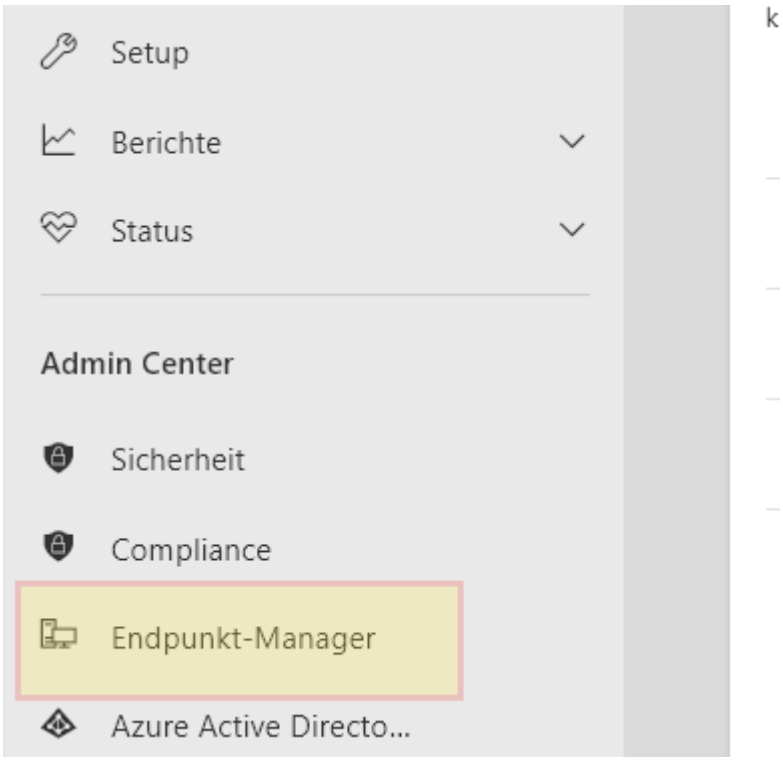




2.2 Microsoft Intune Admin Center (ehemals Endpoint Manager)

Mit den neuem Lizenzmodell (ab Juli 2021) auf Basis von „Microsoft 365 A3“ sind nun auch die Lizenzen für das Gerätemanagement enthalten: „Microsoft Endpoint Manger“, meist nur „Intune“ genannt. Nach dem Login als MS365-Administrator z. B. über https://m365.cloud.microsoft und dem Klick links unten auf das Symbol „Admin“ kommt man in das „Microsoft 365 admin center“, wählt

dort links unten „Alle Anzeigen“ und sieht damit den „neuen“ Menüpunkt „Endpoint Manager“ (= Intune):



Damit gelangen wir zum „normalen“ Microsoft Endpoint Manager (Intune).

Es gibt zwei verschiedene Verwaltungs-Plattformen für Intune:

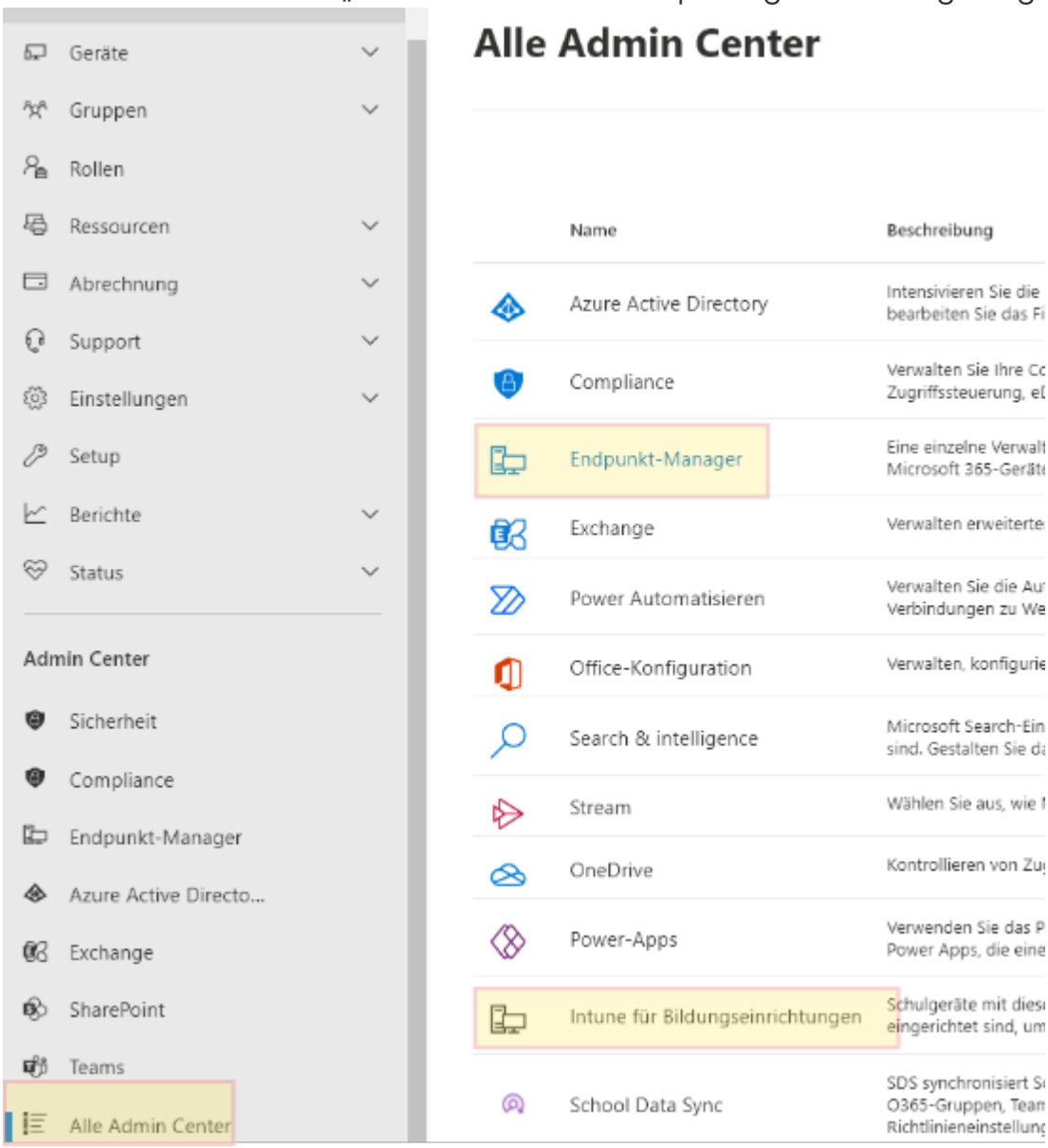
- Intune – Endpoint Manager (voller Funktionsumfang)
- Intune für Bildungseinrichtungen (eingeschränkter Funktionsumfang, aber dafür in manchen Bereichen übersichtlicher)

Es dürfen beide Versionen ohne Einschränkung benutzt werden und Einstellungen, die bei der einen Version gemacht werden, sind natürlich auch bei der anderen Version gültig, da es sich bei den Versionen ja nur um verschiedene Bedienoberflächen handelt.

Wir verwenden meist den „normalen“ Endpoint Manager, wechseln aber ab und zu auch zur Education-Darstellung, weil manche Einstellungen in der Education Variante einfach leichter zu machen sind.

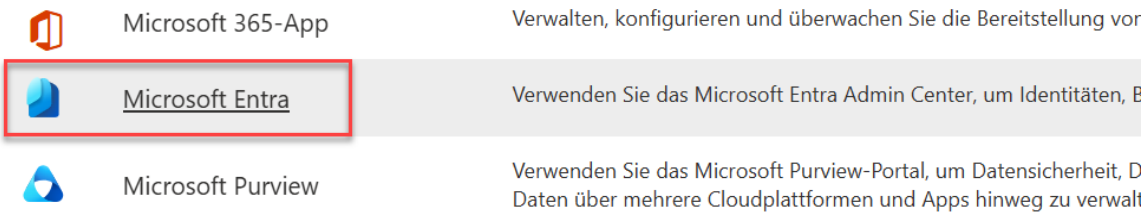
Ein Wechsel zwischen den Versionen ist jeweils über „Alle Dienste“ – Intune bzw. Intune for Education möglich. Man kann aber auch im „Microsoft 365 admin

center“ links unten über „Alle Admin Center“ zur jeweiligen Version gelangen.



2.3 Microsoft Entra (ehemals Azure Active Directory)

Da oder dort kann es auch erforderlich sein, dass wir über das „Azure Active Directory“ Portal auf gewisse Einstellungen zugreifen (z. B. im Bereich „dynamische Gruppen“).



2.4 Wichtige Links zur Verwaltung mit Intune

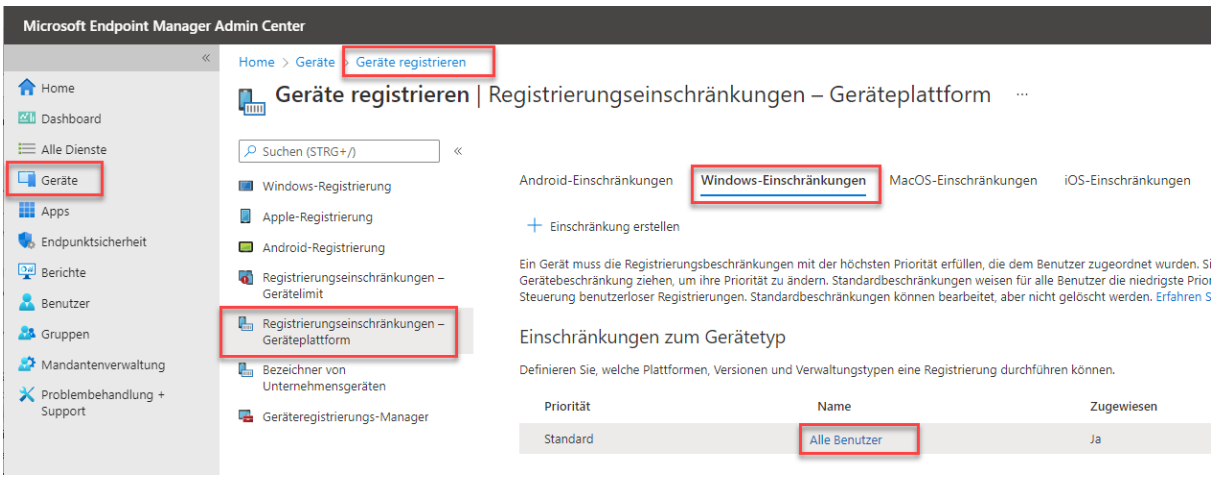
Microsoft Admin Center	https://admin.microsoft.com
Microsoft Intune Admin Center	https://intune.microsoft.com
Microsoft Entra Admin Center	https://entra.microsoft.com

3 Konfiguration und Installation

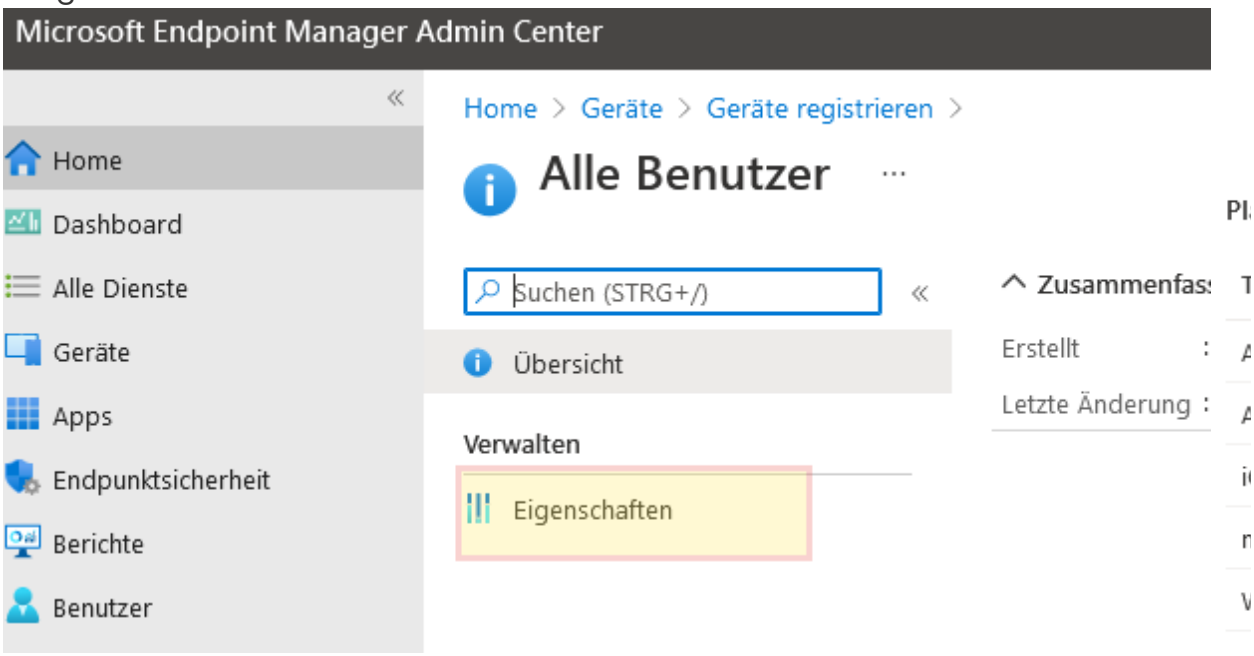
3.1 Privatgeräteregistrierung verhindern

Damit private Geräte im AzureAD nicht registriert werden können, machen wir folgende Einstellung:

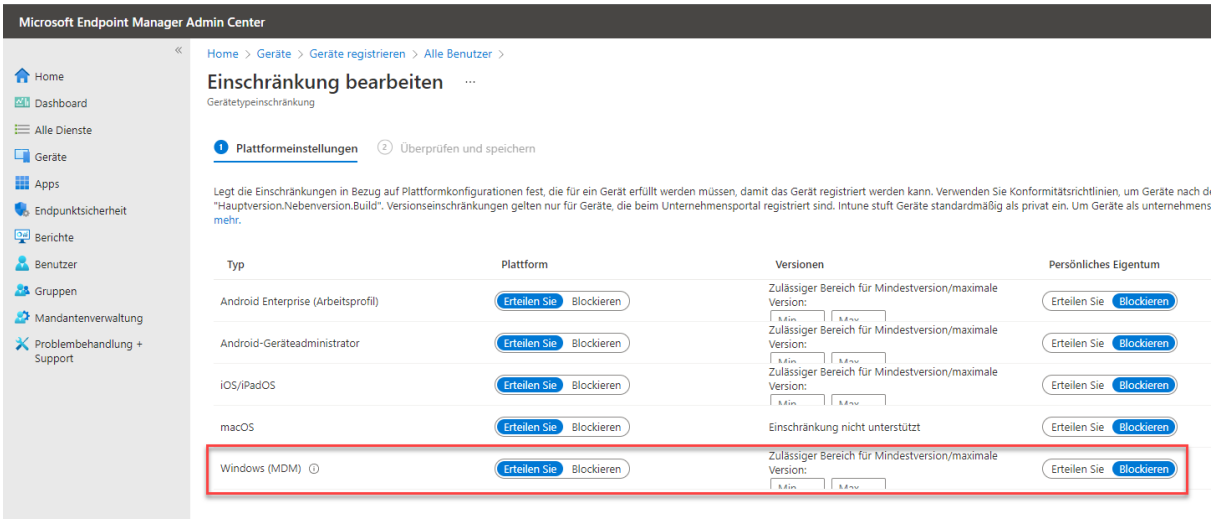
Endpoint Manager (=Intune: https://aka.ms/Intune) > Geräte > Geräte registrieren > Registrierungseinschränkungen > Geräteplattform > Windows-Einschränkungen > Alle Benutzer



> Eigenschaften



Einschränkung bearbeiten:



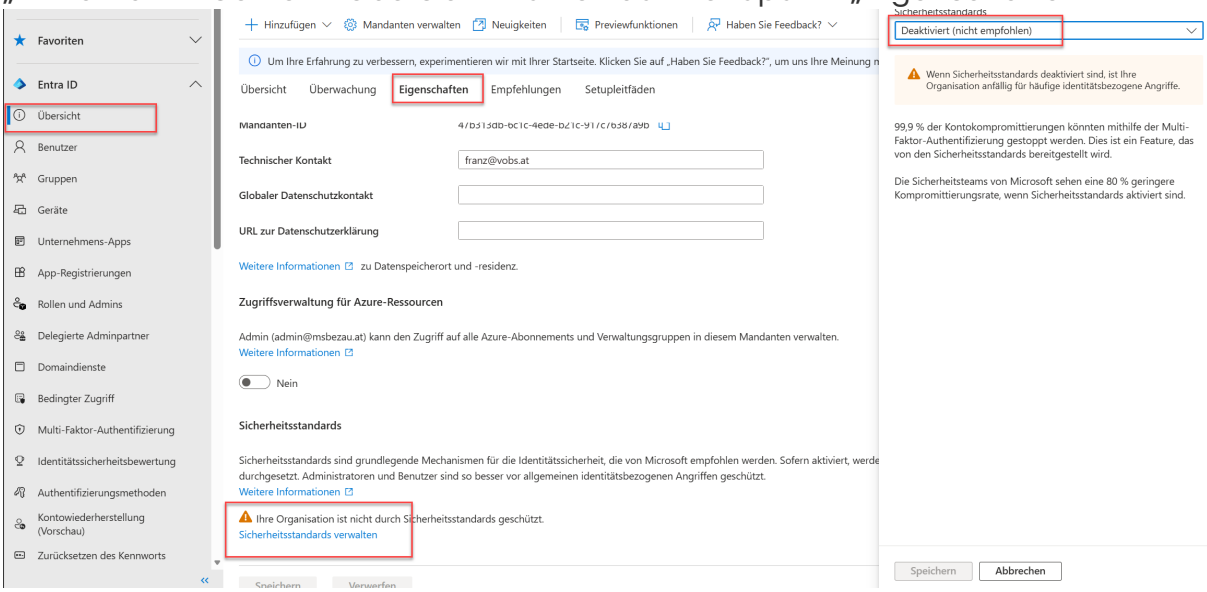
Unter Umständen sind das auch schon die vorgegebenen Standardeinstellungen.

3.2 Multifaktor-Authentifizierung für normale Benutzer deaktivieren

Im Herbst 2021 hat Microsoft wieder einmal im Bereich „Sicherheit“ die Daumenschrauben ohne Ankündigung oder entsprechende Information gehörig angezogen: Beim ersten Login an den Geräten wird eine Zweifaktor-Authentifizierung (mit der App „Microsoft Authenticator“) zwingend gefordert. Das ist in unserem Umfeld nicht praxistauglich.

Über folgende Einstellung kann das deaktiviert werden:

„Entra Admin Center – Übersicht – unten auf Menüpunkt „Eigenschaften“:

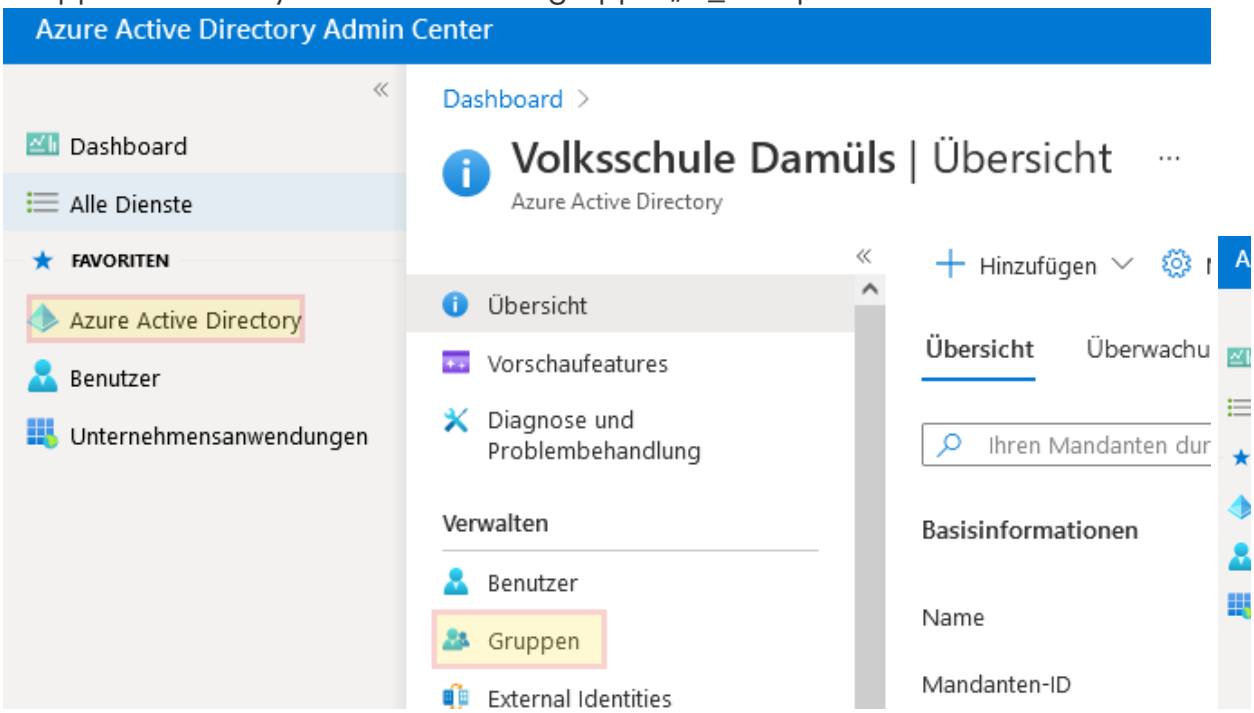


> Umso wichtiger ist die Aktivierung der mehrstufigen Authentifizierung für Admin-Konten!

3.3 Gerätegruppen erstellen:

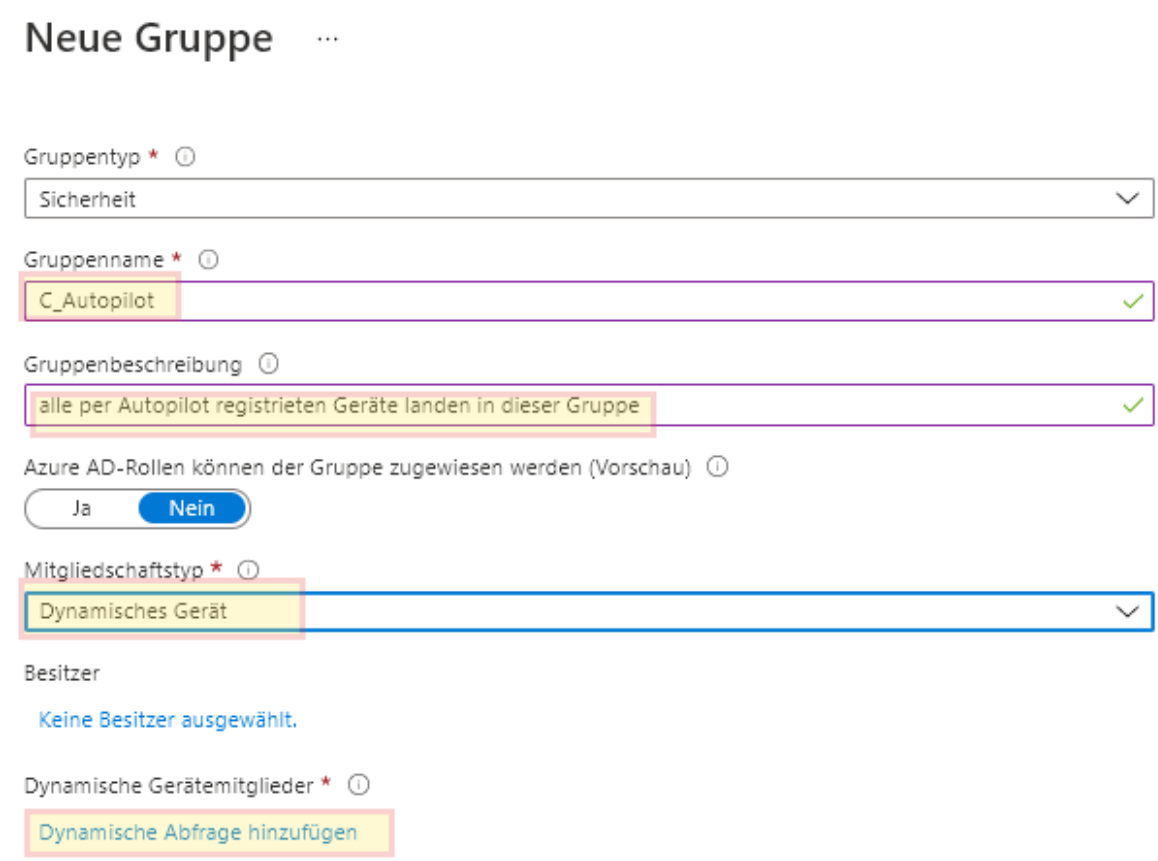
> Entra ADmin Center

Gruppen – neue dynamische Gerätegruppe: „C_Autopilot“

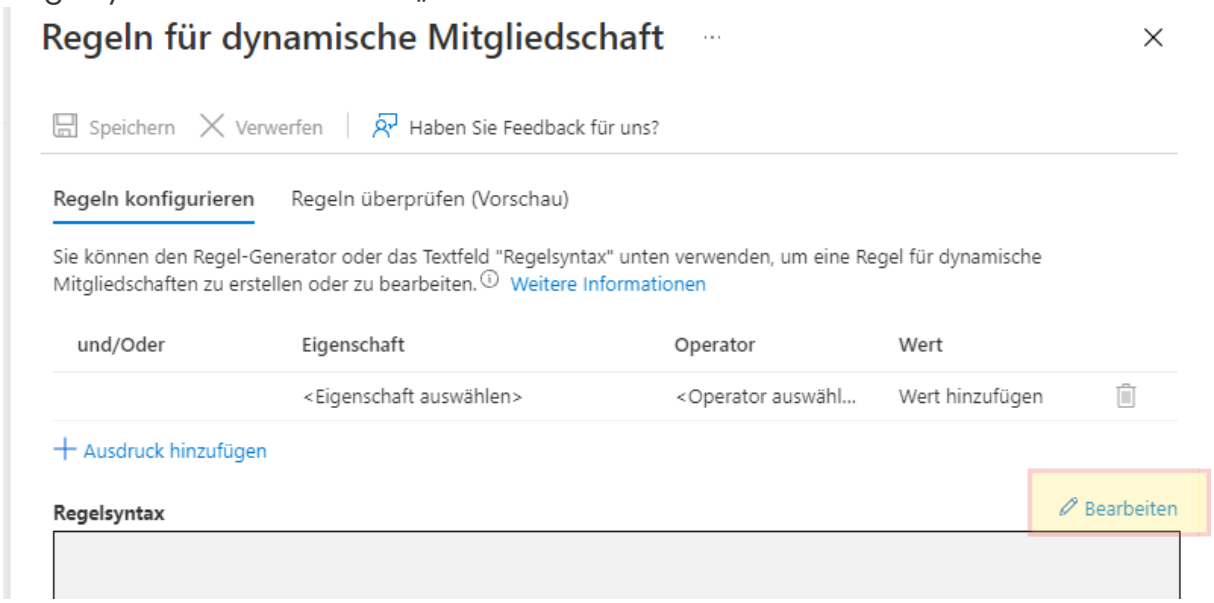


Dynamische Gerätegruppe für alle Autopilot registrierten Geräte
Gruppenname: C_Autopilot

> Analog zu den On-Premises Installationen vom VOBS verwenden wir auch in Intune für alle Gerätegruppen das Präfix “C_” und für alle Benutzergruppen “B_”.



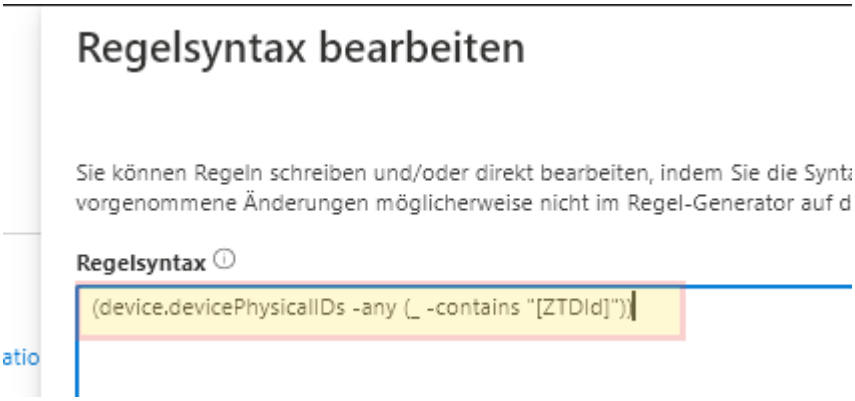
Regelsyntax – rechts unten „Bearbeiten“:



Query kommt von:
https://docs.microsoft.com/en-us/mem/autopilot/enrollment-autopilot

alle Autopilot Geräte sollen automatisch in der Gruppe landen – Query:

```
(device.devicePhysicalIDs -any (_ -contains "[ZTDId]"))
```

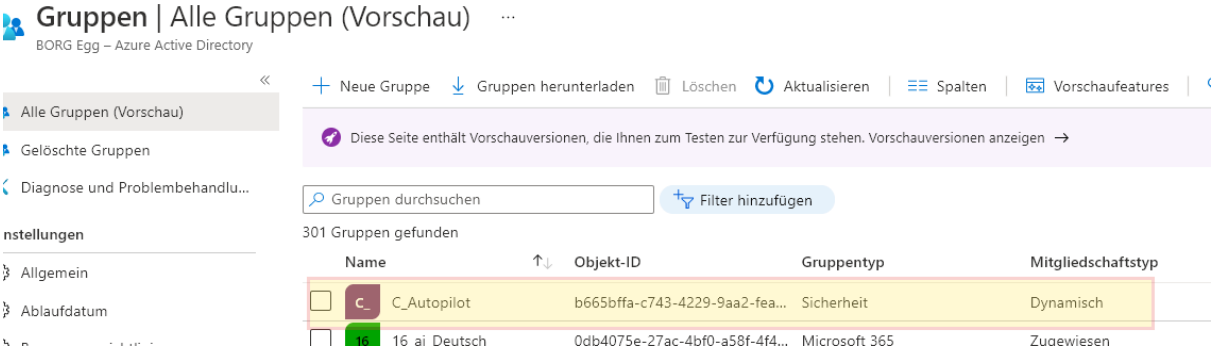


Ok + Speichern > Erstellen

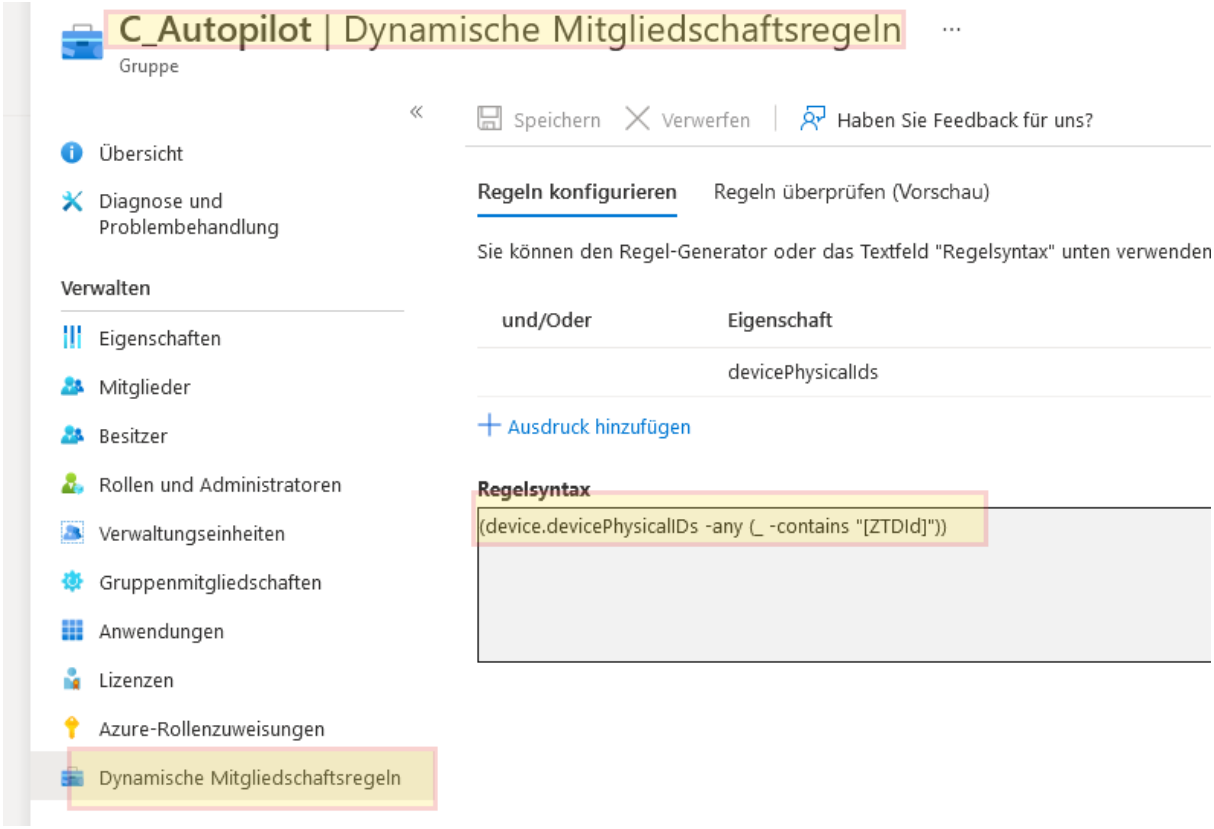
> Beim Kopieren des Query-Strings ist Vorsicht geboten (z. B. Typus der Bindestriche und Anführungszeichen beachten. Die Query-Strings sind hier als Text abrufbar: https://www.vobs.at/fileadmin/user_upload/itservice/downloads/digitaleendgeraete/query.txt

Wenn wir davon ausgehen, dass wir alle Geräte aus der Geräteinitiative per “Autopilot” registrieren, haben wird mit “C_Autopilot” eine Gerätegruppe in der automatisch alle unsere Geräte landen (wichtig dann z.B. beim Zuweisen von Konfigurationsprofilen, Richtlinien, Apps … über diese Gerätegruppe).

Kontrolle:

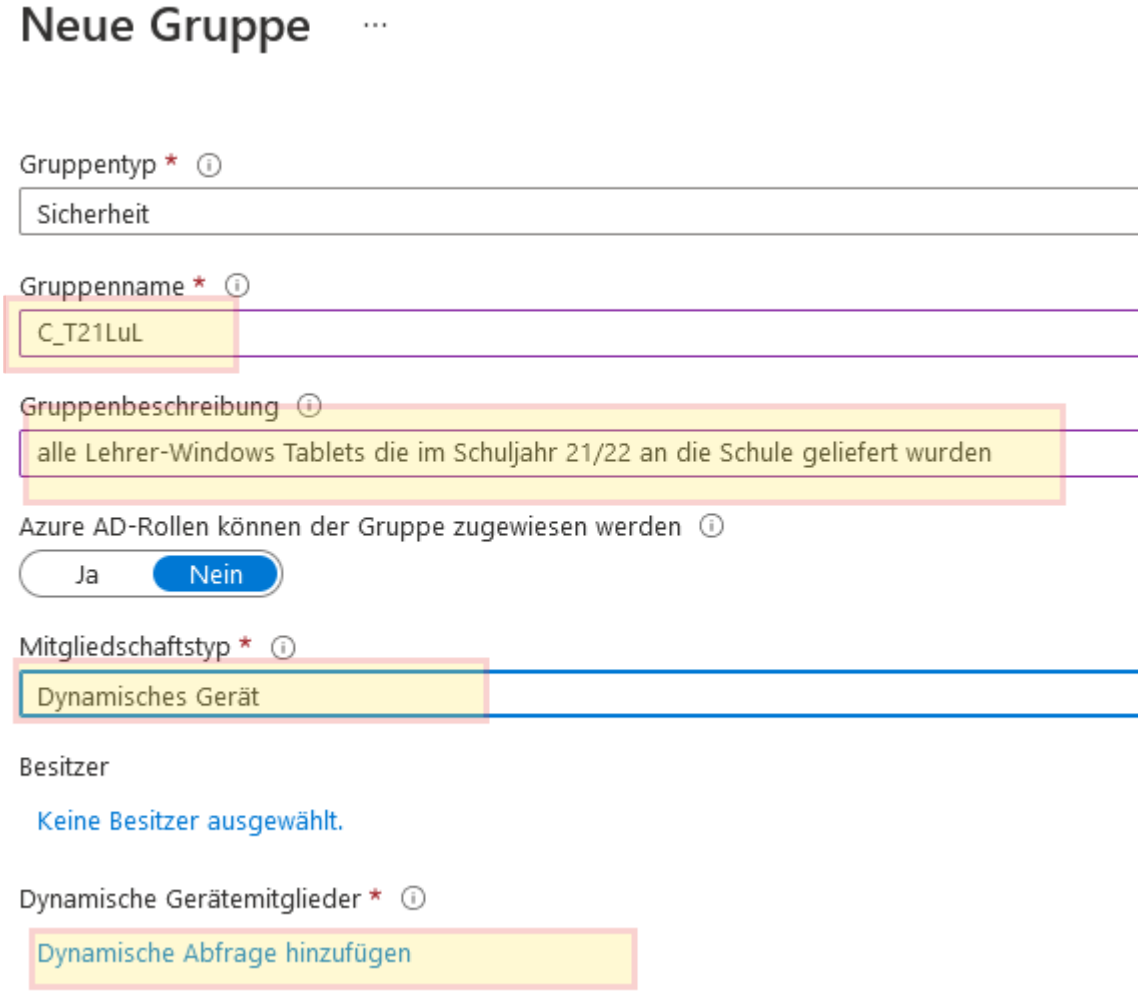


Eigenschaften > Dynamische Mitgliedschaftsregeln



weitere neue dynamische Gerätegruppe: „C_T21LuL“ (bzw. „C_N21LuL“)
Gruppenname: „C_T21LuL“ bzw. „C_N21LuL“ bei Windows-Tablets
Gruppenbeschreibung z. B.: alle Lehrer-Windows Tablets die im Schuljahr 21/22

an die Schule geliefert wurden



Wiederum:

- Dynamische Gerätegruppe
- Dynamische Abfrage – Regelsyntax:

```
(device.devicePhysicalIds -any _ -eq "[OrderID]:T21LuL")
```

> weitere neue dynamische Gerätegruppe: „C_T20SuS“ (bzw. „C_N20SuS“)
Gruppenname: „C_T20SuS“ bzw. „C_N20SuS“ bei Windows-Tablets
Gruppenbeschreibung z. B.: alle Schülertablets von SuS, die im SJ 20/21 an die Schule gekommen sind

Dynamische Abfrage – Regelsyntax:

```
(device.devicePhysicalIds -any _ -eq "[OrderID]:T20SuS")
```

> weitere neue dynamische Gerätegruppe: „C_T21SuS“ (bzw. „C_N21SuS“)

Gruppenname: „C_T21SuS“ bzw. „C_N21SuS“ bei Windows-Tablets
Gruppenbeschreibung z. B.: alle Schülertablets von SuS, die im SJ 21/22 an die Schule gekommen sind

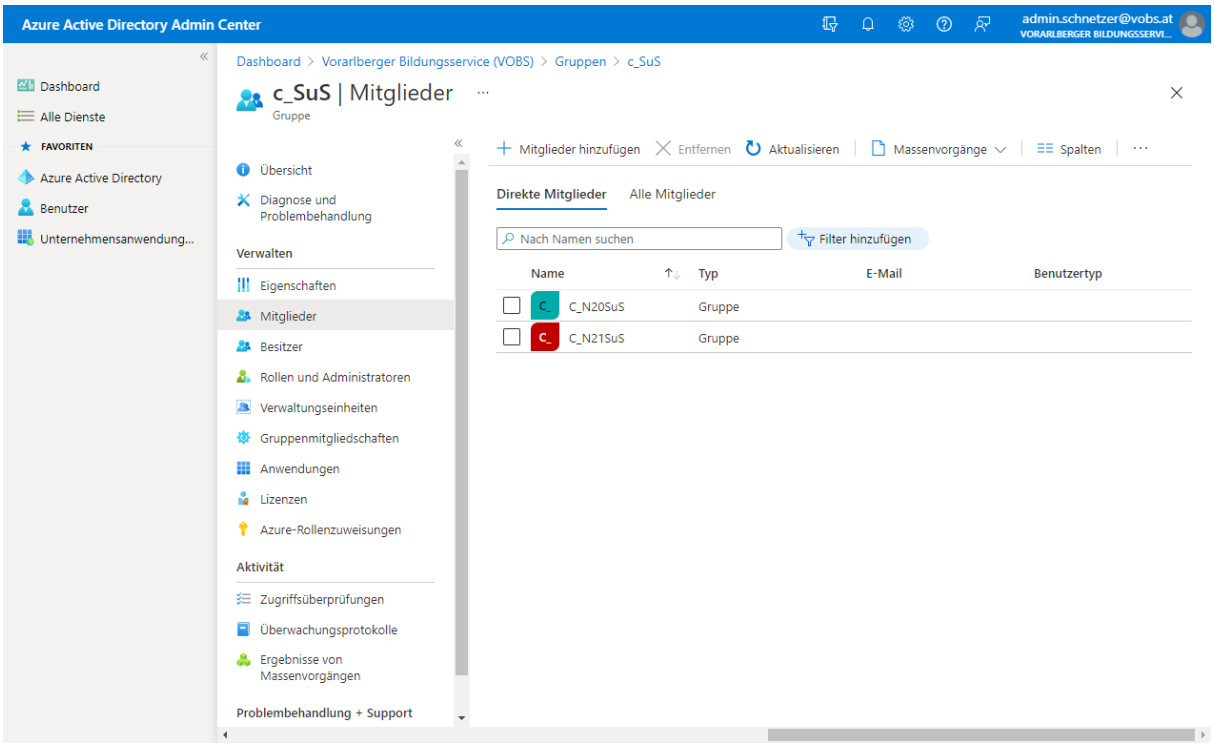
Dynamische Abfrage – Regelsyntax:

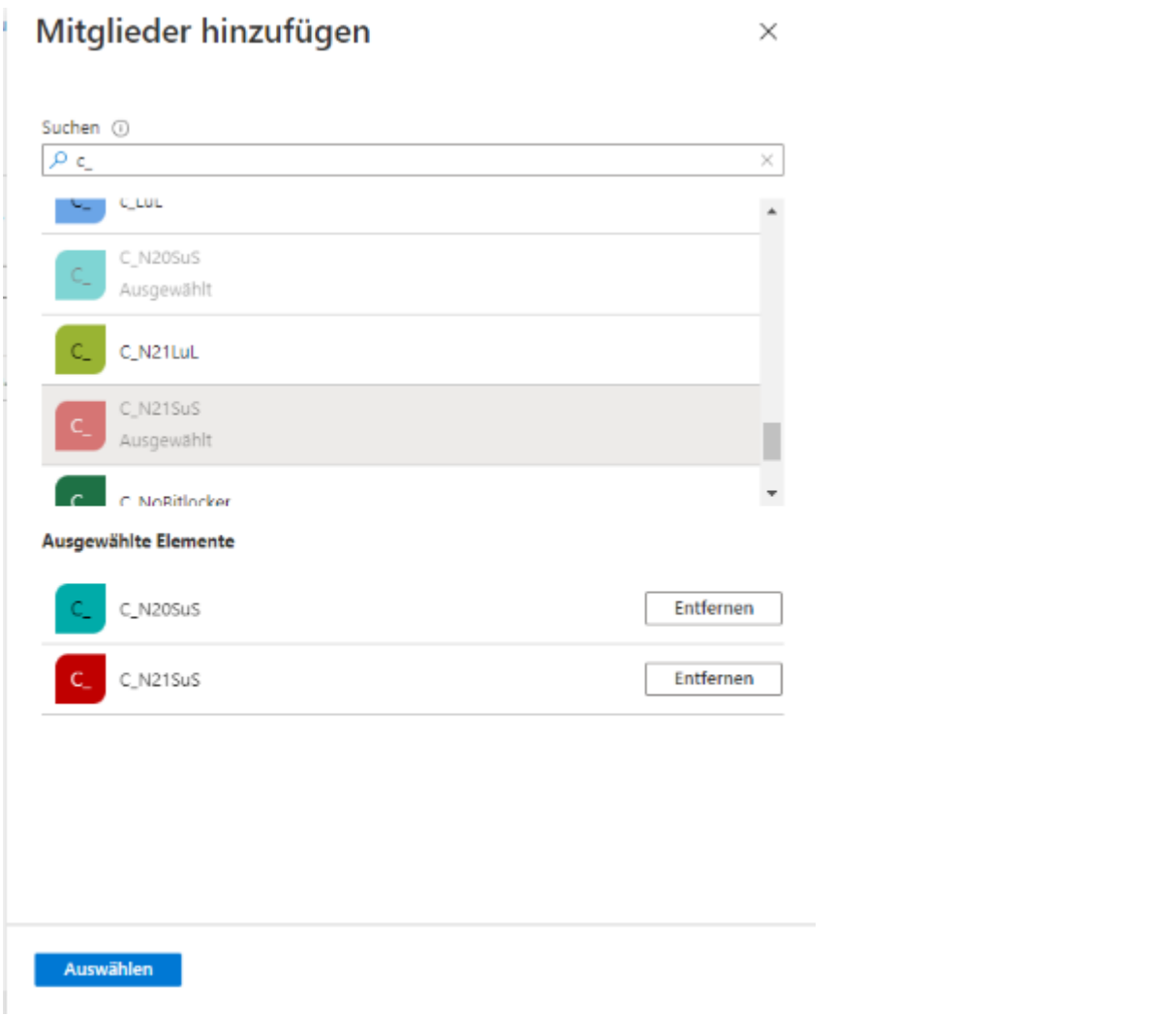
```
(device.devicePhysicalIds -any _ -eq "[OrderID]:T21SuS")
```

Erstellung von statischen LuL und SuS - Gruppen

Wichtig:
Mitgliedstyp: Zugewiesen

Gruppenname: „C_SuS“ bzw. „C_LuL“
Gruppenbeschreibung z. B.: “alle Schülergeräte der Schule” bzw. “alle Lehrergeräte der Schule”
Unter dem Punkt Mitglieder, werden nun die bereits erstellten Gruppen hinzugefügt (analog in der C_LuL-Gruppe)


Azure Active Directory Admin Center
admin.schnetzer@vobs.at
VORARLBERGER BILDUNGSSERVI...
Dashboard
Alle Dienste
FAVORITEN
Azure Active Directory
Benutzer
Unternehmensanwendung...
Dashboard > Vorarlberger Bildungsservice (VOBS) > Gruppen > c_SuS
c_SuS | Mitglieder
Gruppe
Übersicht
Diagnose und Problembehandlung
Verwalten
Eigenschaften
Mitglieder
Besitzer
Rollen und Administratoren
Verwaltungseinheiten
Gruppenmitgliedschaften
Anwendungen
Lizenzen
Azure-Rollenzuweisungen
Aktivität
Zugriffsüberprüfungen
Überwachungsprotokolle
Ergebnisse von Massenvorgängen
Problembehandlung + Support
Mitglieder hinzufügen
Entfernen
Aktualisieren
Massenvorgänge
Spalten
Direkte Mitglieder
Alle Mitglieder
Nach Namen suchen
Filter hinzufügen
Name
Typ
E-Mail
Benutzertyp
C_N20SuS
Gruppe
C_N21SuS
Gruppe

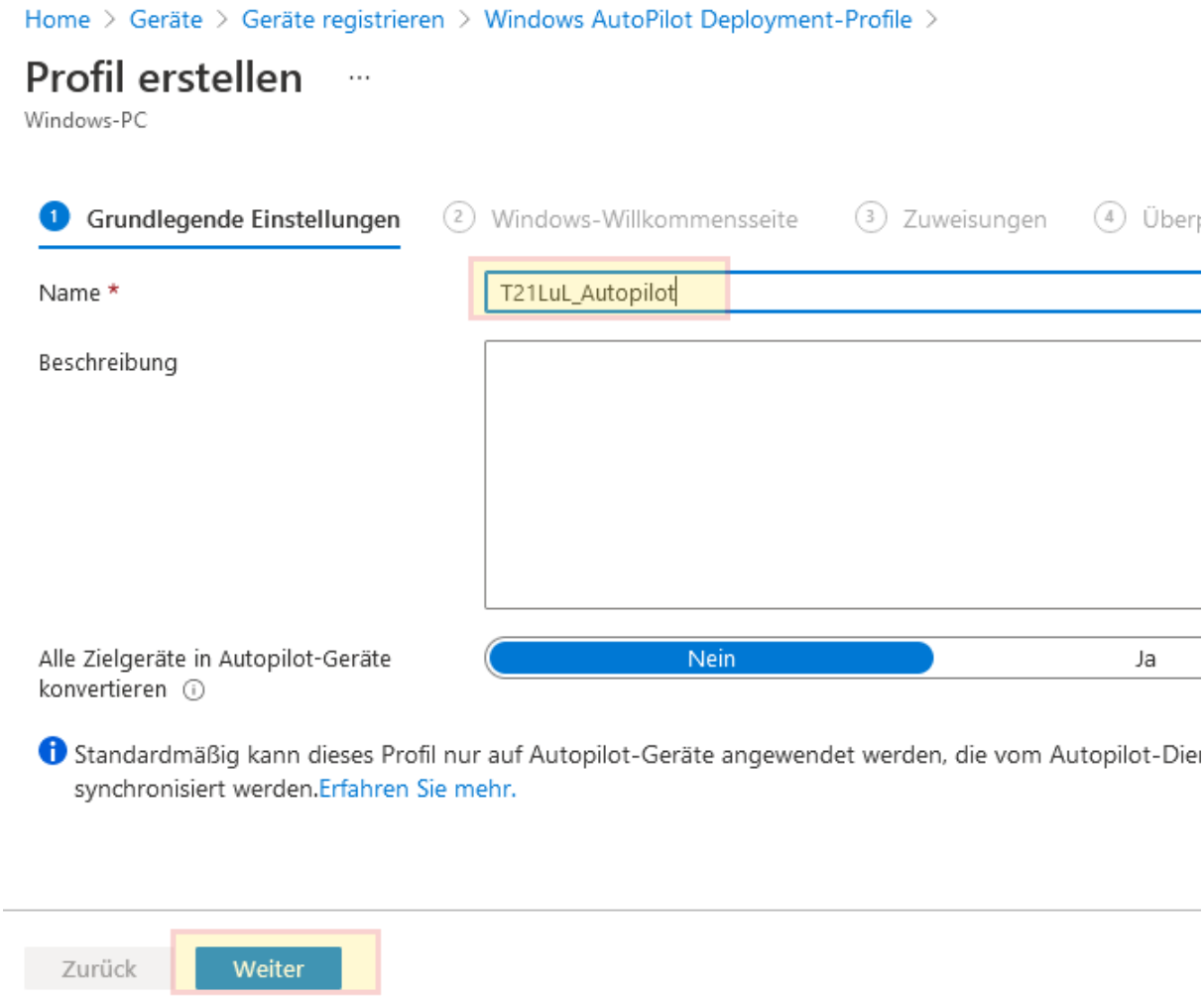

Mitglieder hinzufügen
Suchen
c_
C_N20SuS
Ausgewählt
C_N21LuL
C_N21SuS
Ausgewählt
Ausgewählte Elemente
C_N20SuS
Entfernen
C_N21SuS
Entfernen
Auswählen

3.4 Autopilot-Profile erstellen:

Für jede Gerätegruppe (bzw. für jeden Gruppentag vom CSV-Importfile) legen wir ein eigenes Autopilot-Profil an:

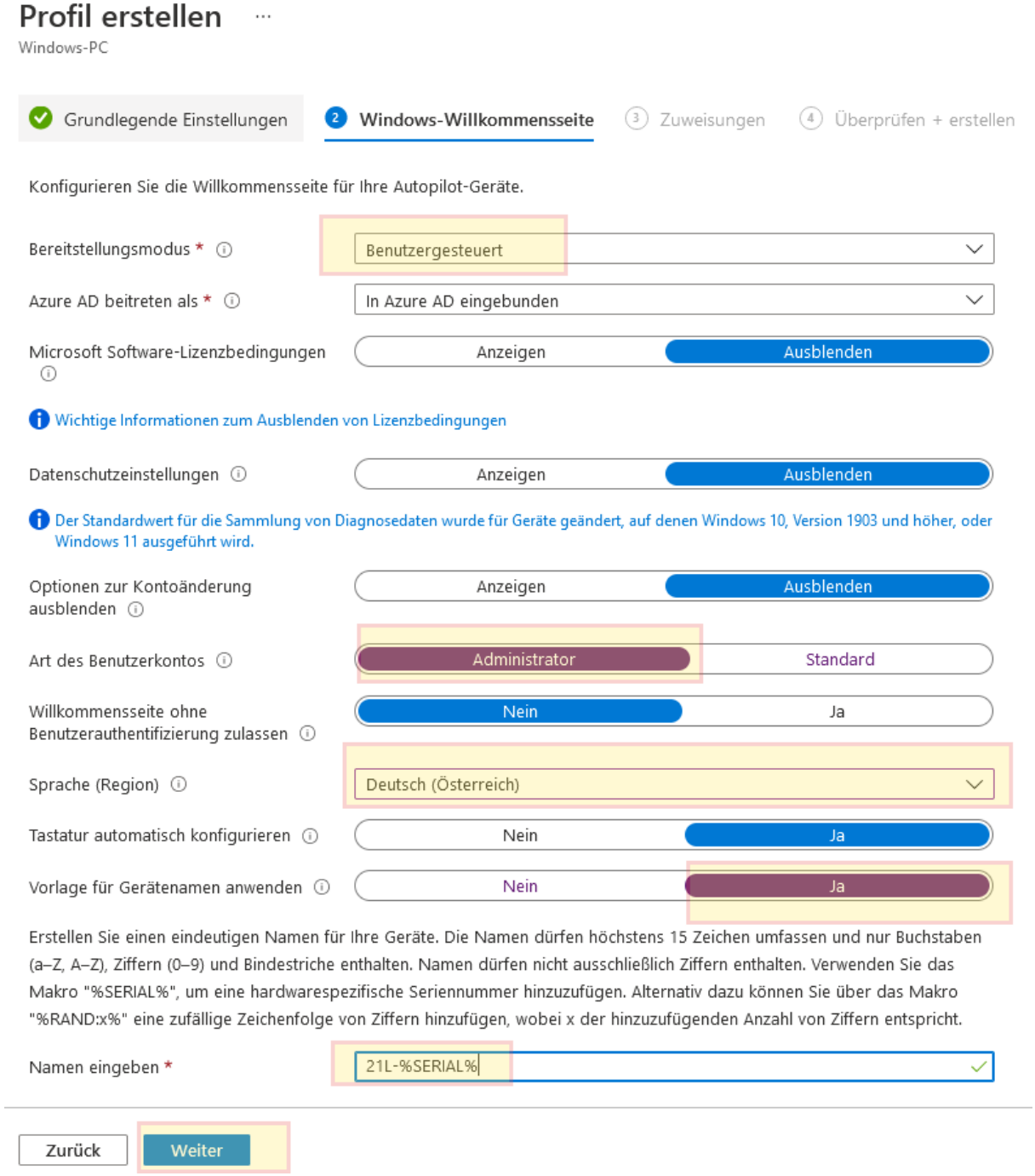
Intune – Geräte – Geräte registrieren – Bereitstellungsprofile:
„Profil erstellen“ – „Windows-PC“

Profilname: „T21LuL_Autopilot“ bzw. „N21LuL_Autopilot“



Beschreibung z. B.: Lehrergeräte Schuljahr 2021 2022

Option 1:
Windows-Willkommensseite – bei LuL: „Benutzergesteuert“

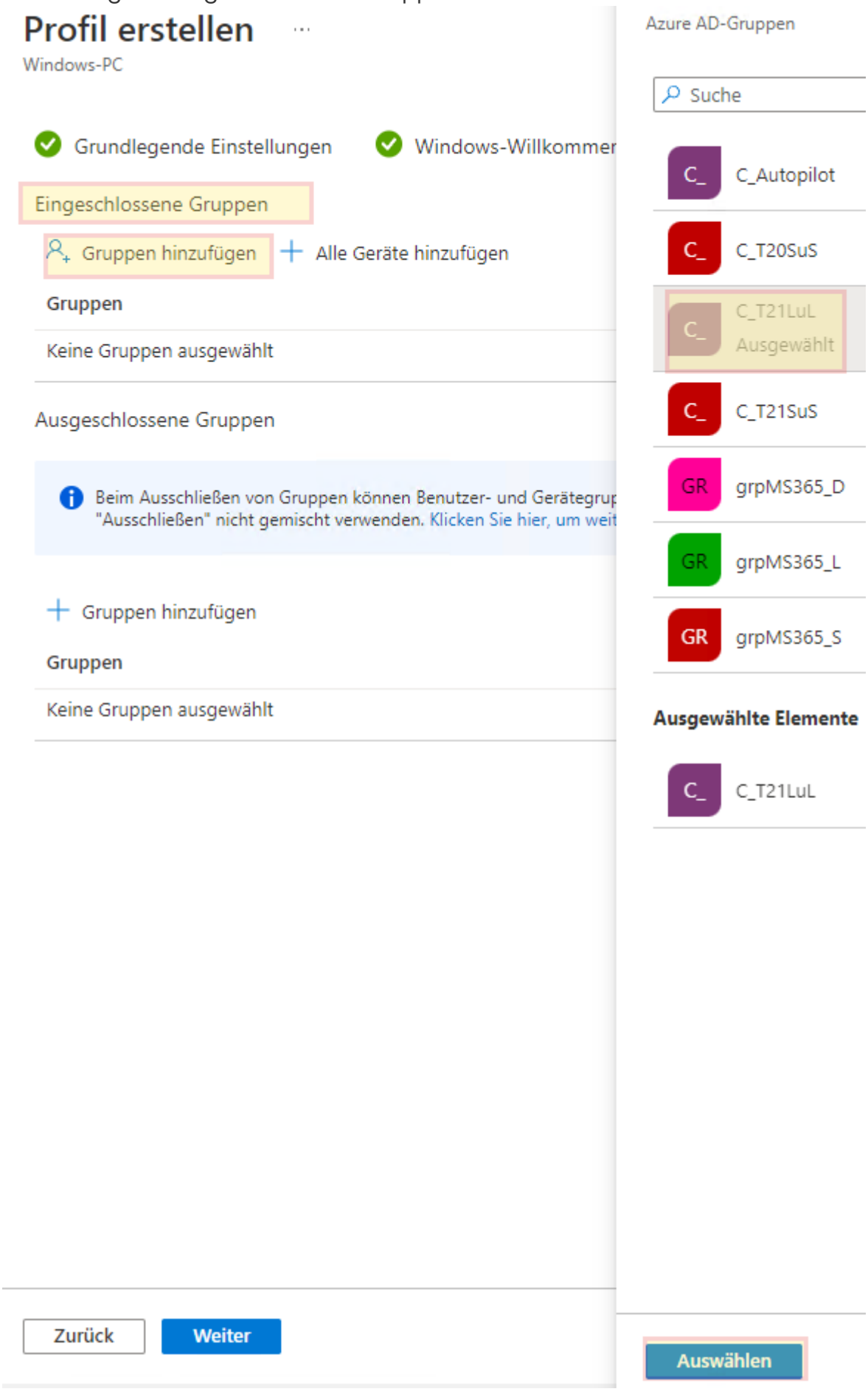


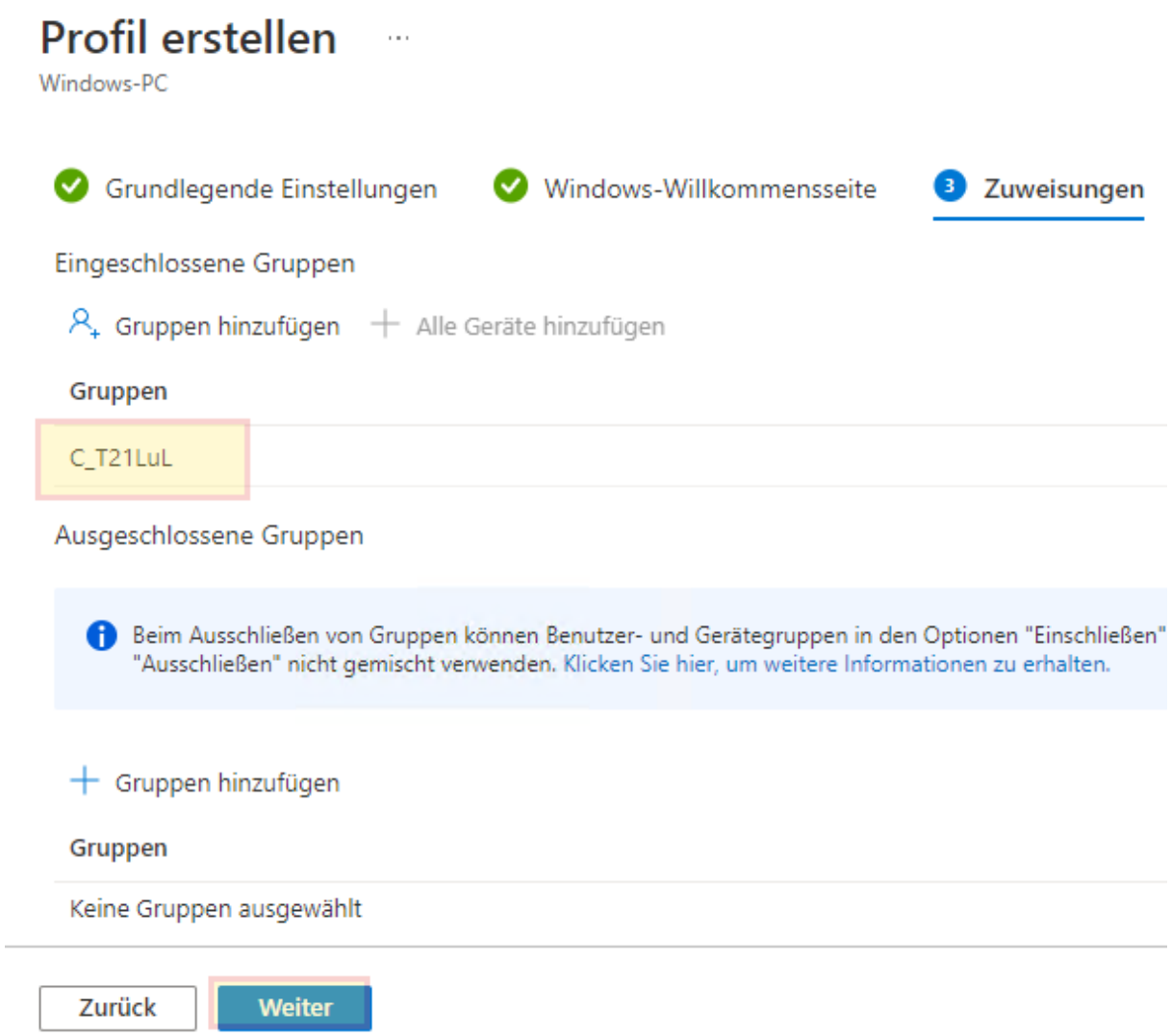
Namen eingeben: 21L-%SERIAL%

Option 2:
Änderung bei “Art des Benutzerkontos” auf Standard.

> Wir machen bei den Lehrergeräten den ersten Benutzer (= MS365-Login) hier zum Administrator (nur bei Option 1), damit die LuL die Möglichkeit bekommen, einen privaten Drucker etc. zu Hause zu installieren.

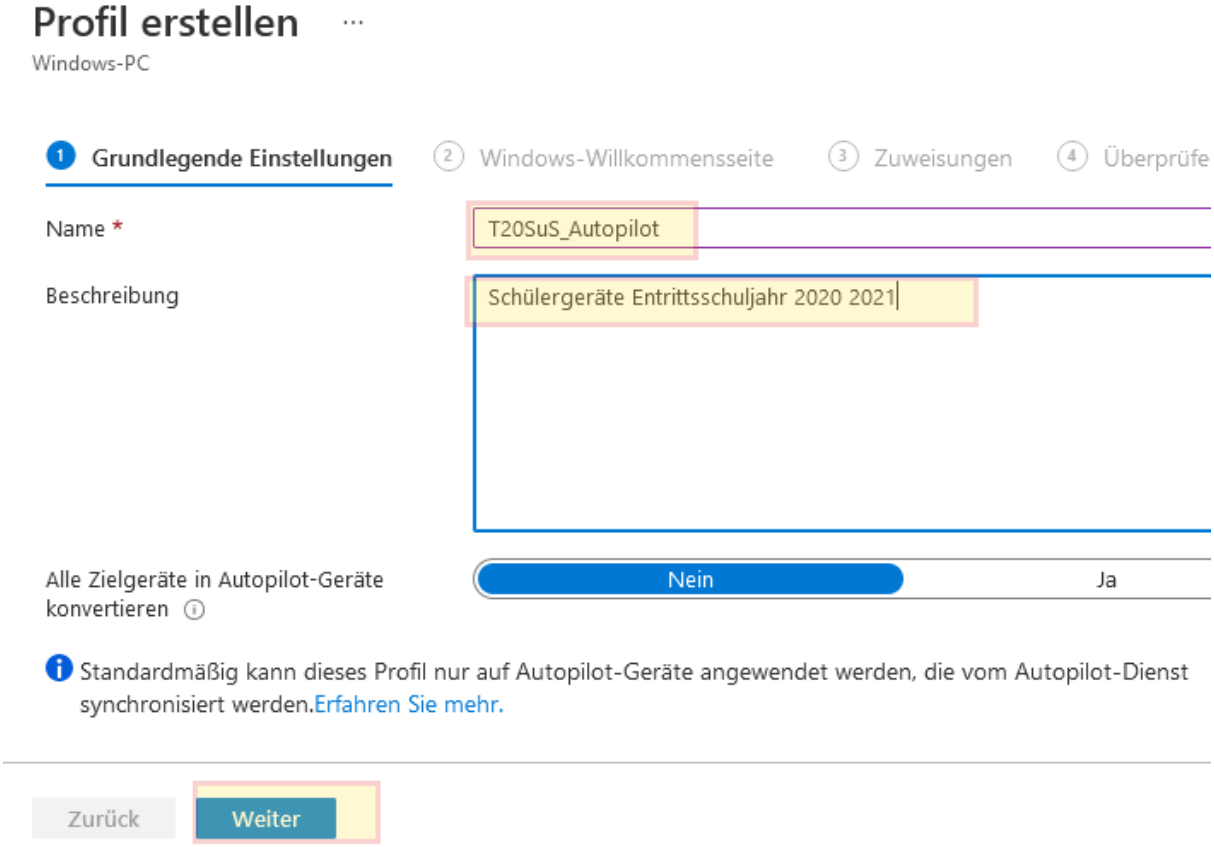
Zuweisungen - Eingeschlossene Gruppen:




Profil erstellen
Windows-PC
Grundlegende Einstellungen
Windows-Willkommensseite
3 Zuweisungen
Eingeschlossene Gruppen
Gruppen hinzufügen
Alle Geräte hinzufügen
Gruppen
C_T21LuL
Ausgeschlossene Gruppen
Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen in den Optionen "Einschließen" "Ausschließen" nicht gemischt verwenden. Klicken Sie hier, um weitere Informationen zu erhalten.
Gruppen hinzufügen
Gruppen
Keine Gruppen ausgewählt
Zurück
Weiter

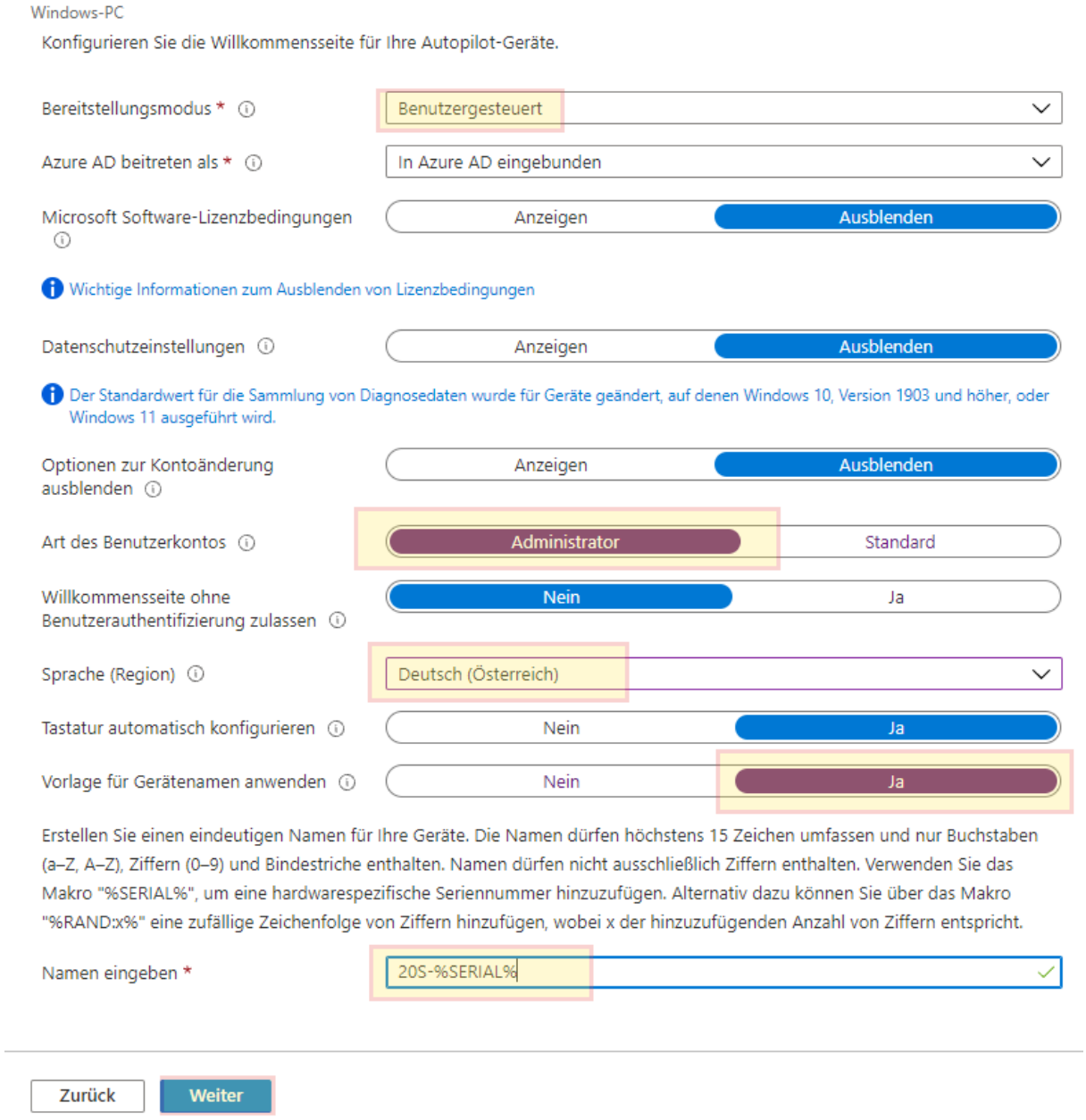
> Erstellen

Windows-PC: Profilname: „T20SuS_Autopilot“ bzw. „N20SuS_Autopilot“
„Profil erstellen“ – „Windows-PC“

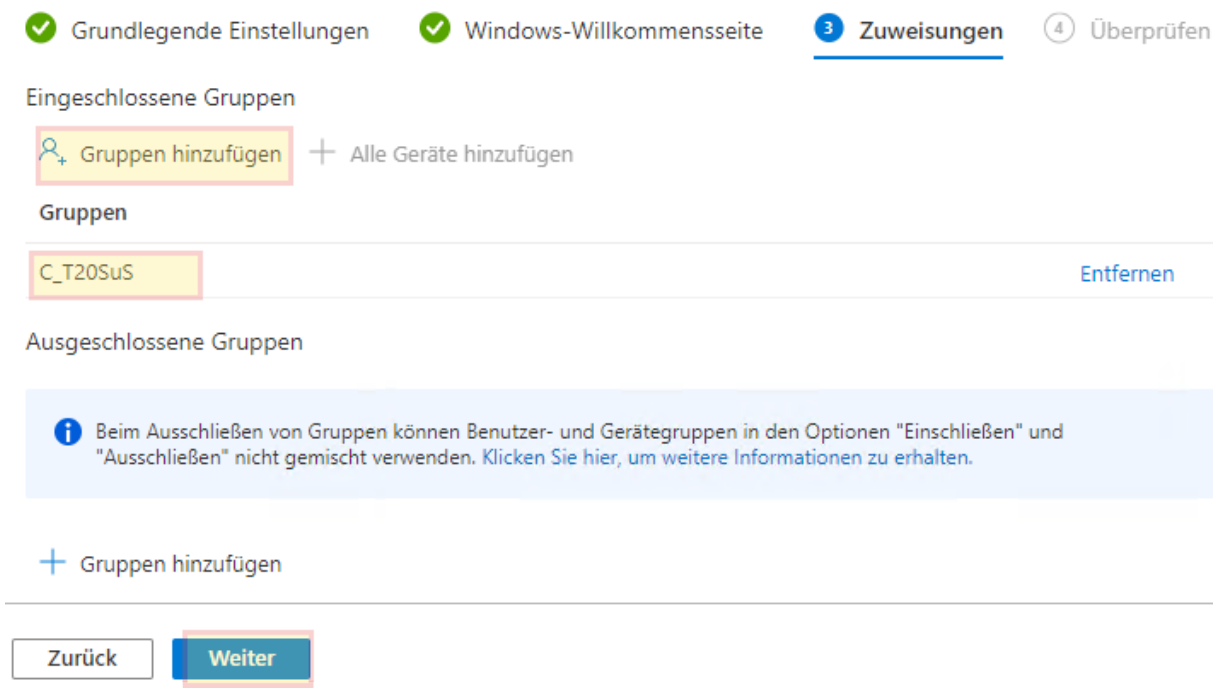


Name: T20SuS_Autopilot
Beschreibung: Schülergeräte Eintrittsschuljahr 2020 2021

Windows-Willkommensseite – bei SuS „Benutzergesteuert“



Namen ergeben: 20S-%SERIAL%
Eingeschlossene Gruppen: „C_T20SuS“



> Erstellen

> Der erste Benutzer (und nur der erste!), welcher sich am Gerät mit seinem Office365 Account anmeldet, wird zum lokalen Administrator des Gerätes gemacht. Dadurch bekommen die SuS überhaupt die Möglichkeit, den lokalen Administrator zu aktivieren und ein persönliches Passwort zu vergeben (oder einen neuen Benutzer „Admin“ anzulegen).

Erstes To-do somit für den Unterrichtsgegenstand „Digitale Grundbildung (nachdem die Geräte verteilt wurden):

Gleich nach dem ersten Login sollen die SuS:

- sich mit ihrem eigenen MS-365-Account anmelden, damit sie vorab einmal lokale Adminrechte haben
- als angemeldeter MS-365-User (hat in diesem Moment noch lokale Adminrechte):
  - lokalen Administrator aktivieren (oder neuen Benutzer mit Adminrechten anlegen)
  - persönliches Passwort für diesen Administrator vergeben (und merken/aufschreiben)
- abmelden und als lokaler Administrator mit dem gerade vergebenen Passwort anmelden
  - MS365-Benutzer zum Standardbenutzer auf dem Gerät machen
  - wieder abmelden und als MS-365-User anmelden (das ist dann der Standarduser mit dem tagtäglich gearbeitet wird)

Analog dazu das dritte Autopilot-Profil erstellen:

Windows-PC: Profilname: „T21SuS_Autopilot“ bzw. „N21SuS_Autopilot“
Name: T21SuS_Autopilot
Beschreibung: Schülergeräte Eintrittsschuljahr 2021 2022
Gerätenamen: 21S-%SERIAL%
Eingeschlossene Gruppen: C_T21SuS

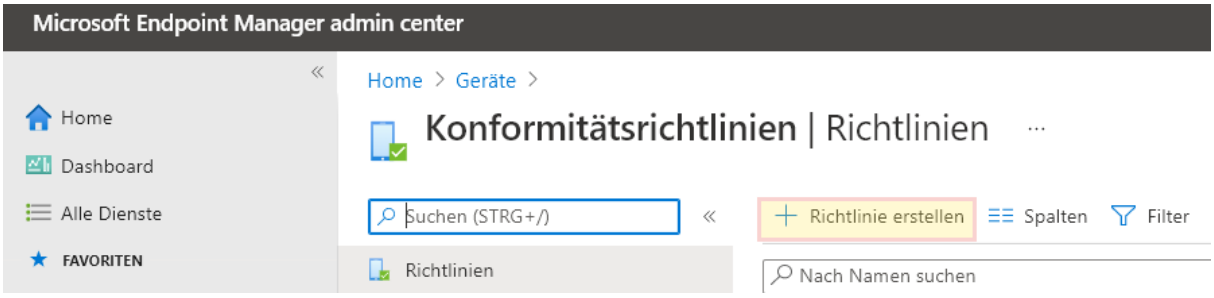
Kontrolle:

Bei „Zugewiesen kann es etwas dauern, bis „Ja“ angezeigt wird (Menüpunkt neu aufrufen).

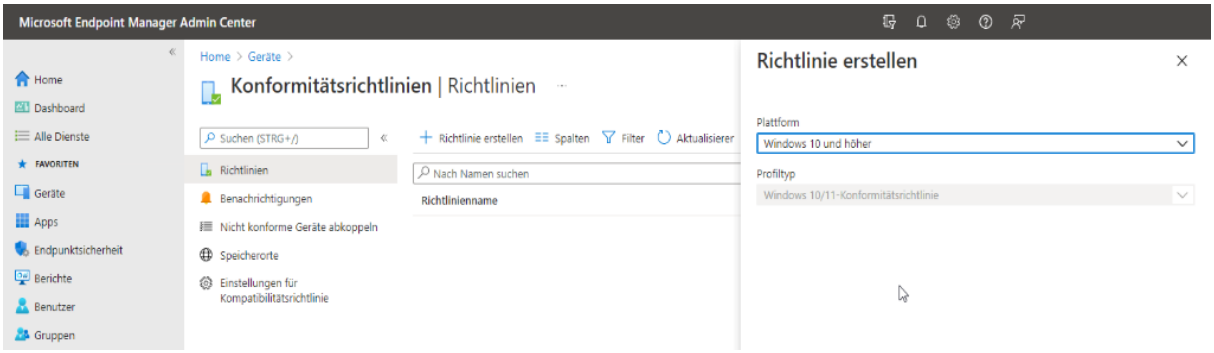
4 Richtlinien und Konfigurationen:

4.1 Konformitätsrichtlinien

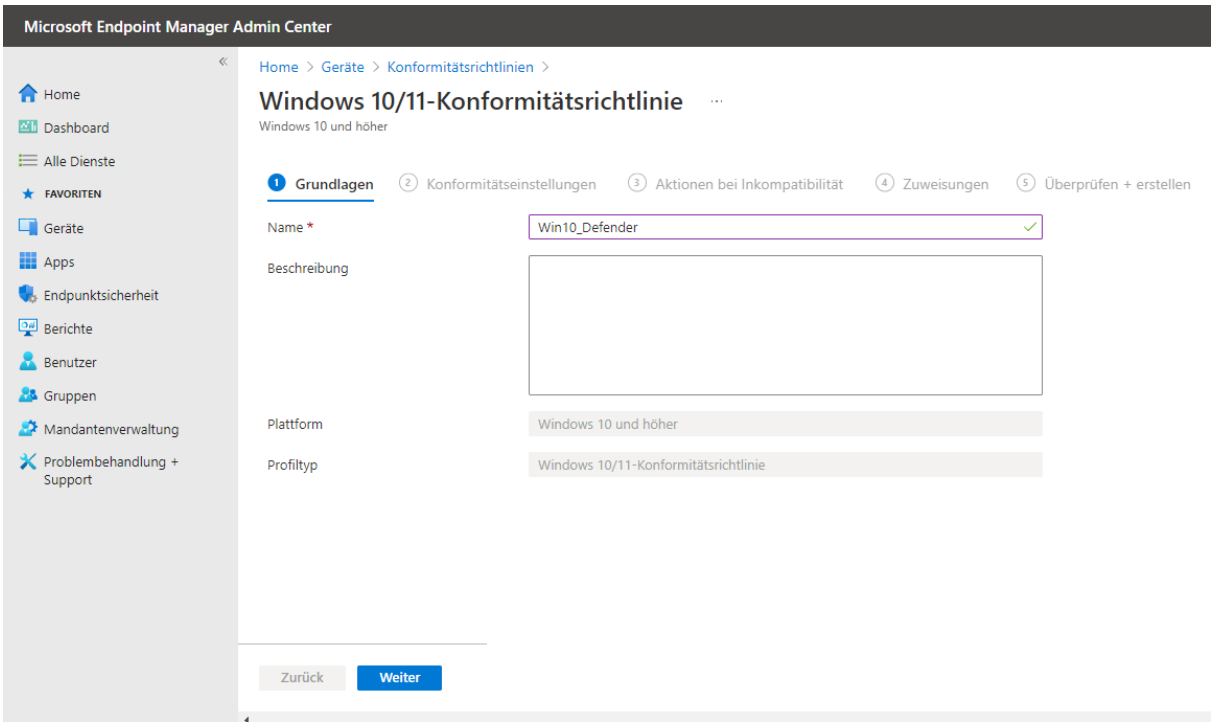
Intune – Geräte - Konformitätsrichtlinien:



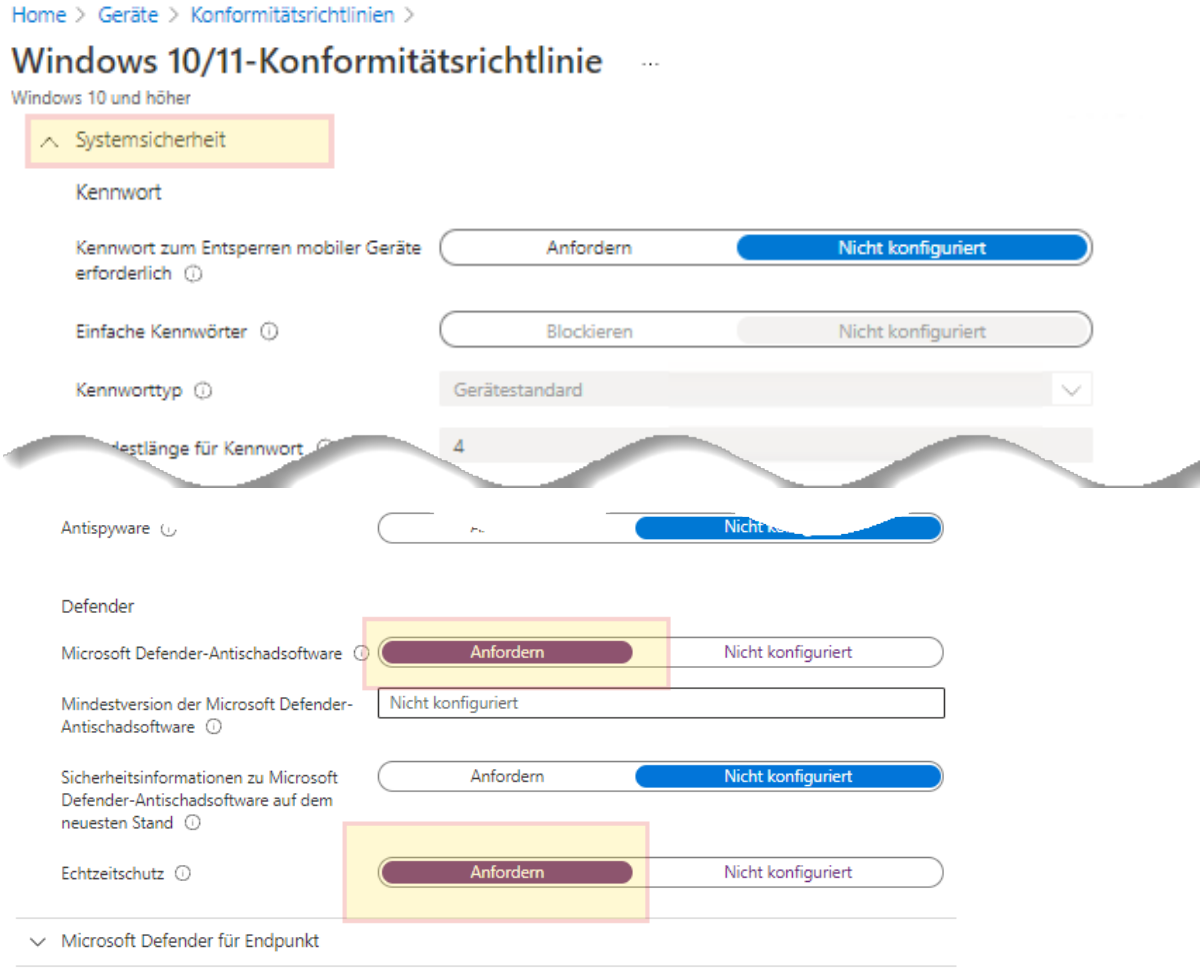
> Erstellen



Plattform: Windows 10 oder höher > Erstellen

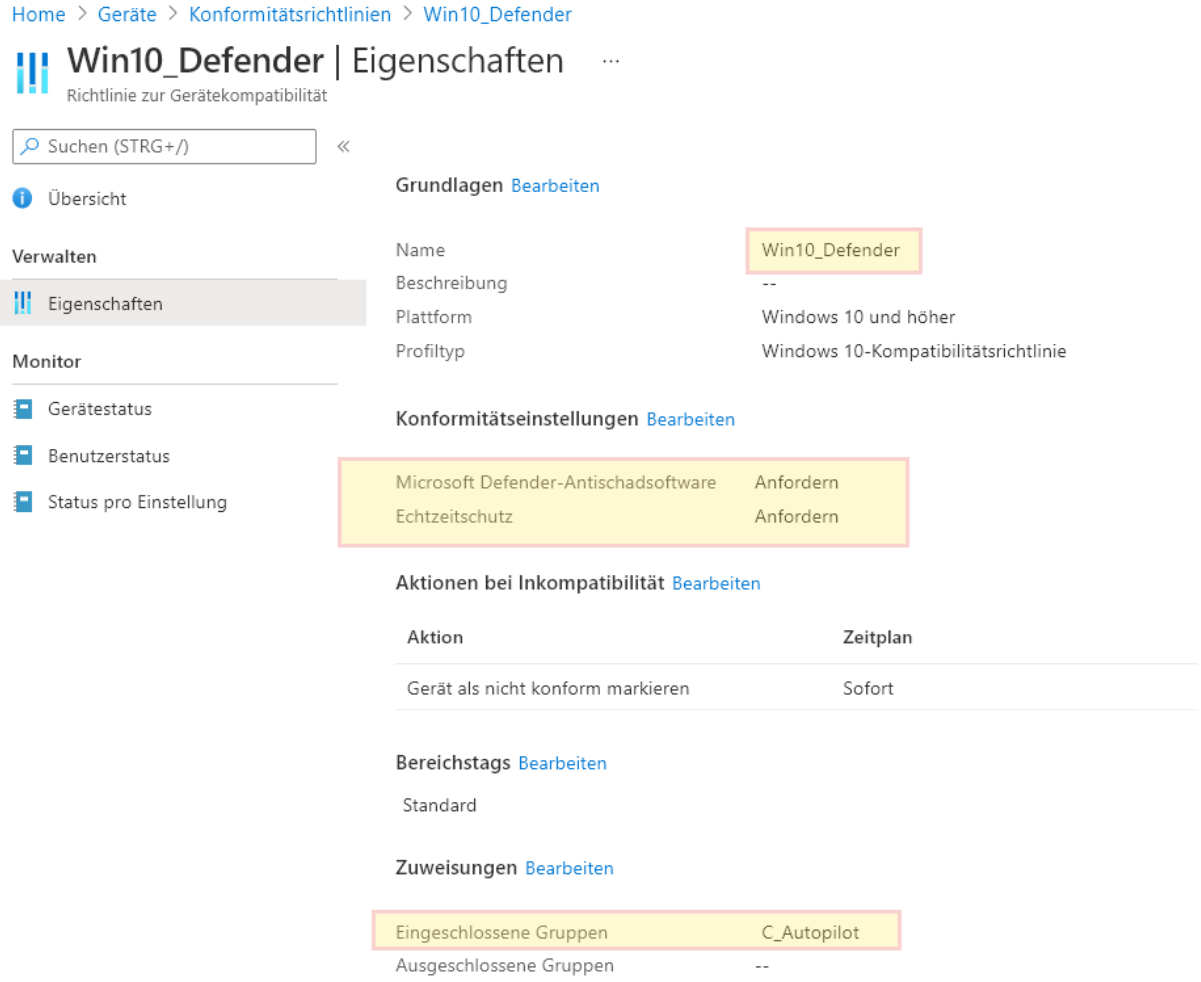


Name: Win10_Defender > Weiter



> weiter > Weiter > bei „Zuweisung“: „eingeschlossene Gruppen: „C_Autopilot“ > Weiter > Erstellen

Kontrolle: Konformitätsrichtlinie auswählen > Eigenschaften:



4.2 Konfigurationsprofile

Intune – Geräte - Konfigurationsprofile:

4.2.1 Optional: Änderung beim Profil „Standardrichtlinien für EDU“

Die Konfiguration der Startseite für Microsoft Edge ist in der Anleitung 02_Intune4Windows_optionale-Konfigurationen nachzulesen.
Richtlinie ist per Default allen Geräten“ zugewiesen – siehe:

4.2.2 Neues Konfigurationsprofil erstellen: WLAN

Damit sich die Geräte nach dem ersten „Internetkontakt“ und dem darauffolgenden Reboot automatisch mit der „richtigen“ und „produktiven“ Wlan-Wolke verbinden, erstellen wir ein eigenes WLan-Profil:
Profil erstellen – rechts oben Plattform auswählen: „Windows 10 oder höher“ – Vorlagen: „WLAN“

Profil erstellen

Plattform

Windows 10 und höher

Profiltyp

Vorlagen

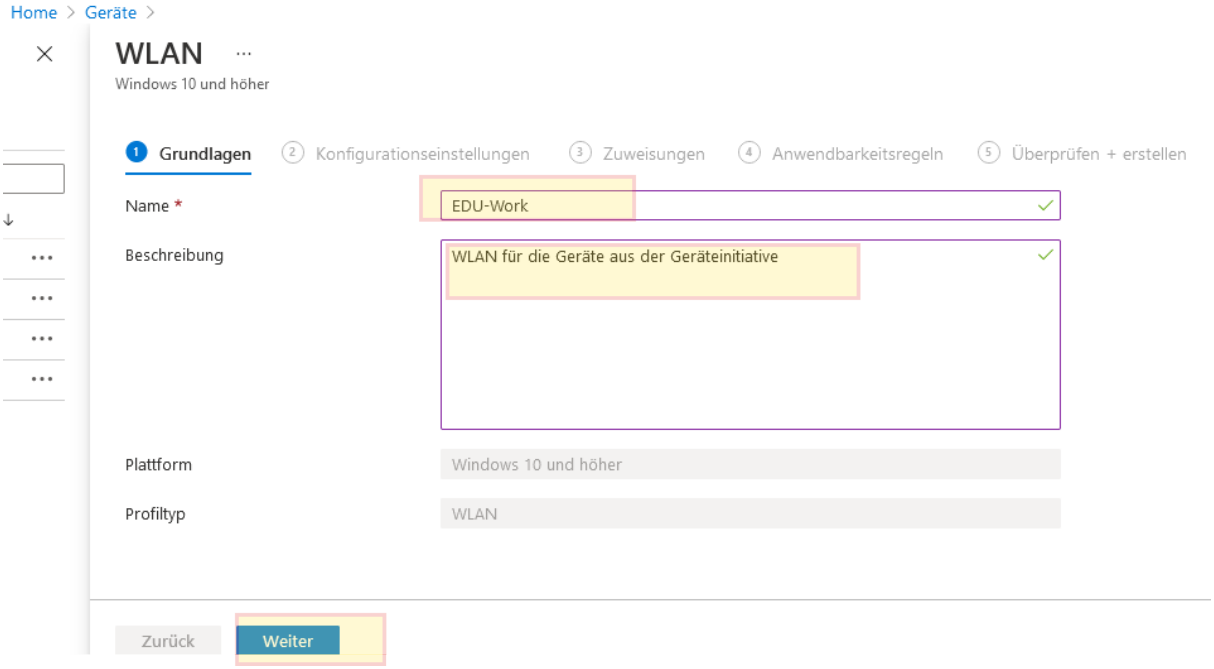
Vorlagen enthalten Gruppen von Einstellungen, die nach Fur
Verwenden Sie eine Vorlage, wenn Sie Richtlinien nicht manu
Zugriff auf Unternehmensnetzwerke konfigurieren möchten,
WLAN oder VPN. Weitere Informationen

Suchen

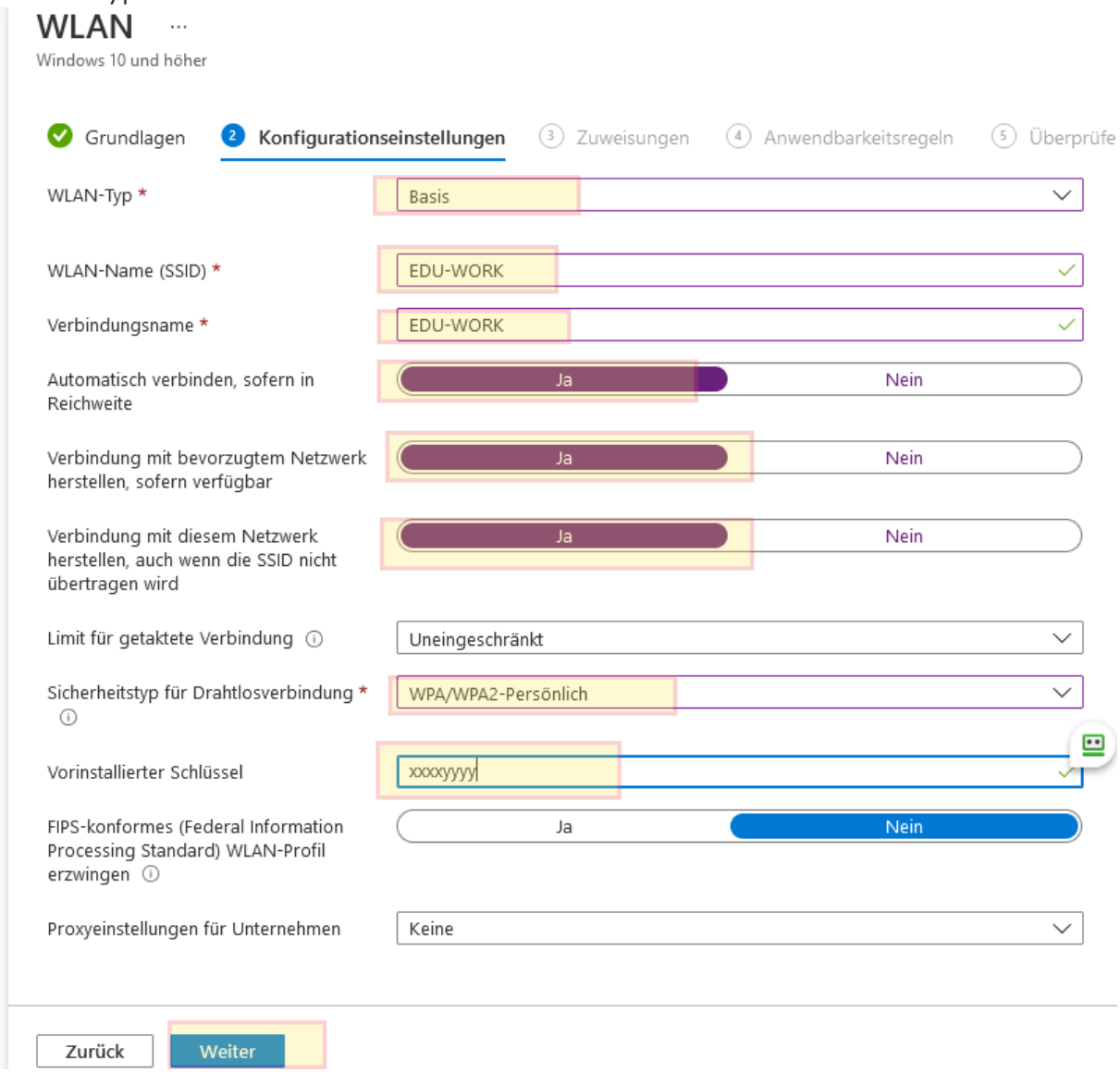
Name der Vorlage
Administrative Vorlagen
Benutzerdefiniert
Domänenbeitritt
E-Mail
Editionsupgrade und Moduswechsel
Endpoint Protection
Freigegebenes, von mehreren Benutzern verwendetes Gerä
Geräteeinschränkungen
Geräteeinschränkungen (Windows 10 Team)
Identity Protection
Importiertes PKCS-Zertifikat
Kiosk
Microsoft Defender für Endpunkt (Windows 10 Desktop)
Netzwerkgrenze
PKCS-Zertifikat
SCEP-Zertifikat
Schnittstelle zur Konfiguration der Gerätefirmware
Sicheres Assessment (Education)
Übermittlungsoptimierung
Vertrauenswürdiges Zertifikat
VPN
Windows-Integritätsüberwachung
WLAN

Erstellen

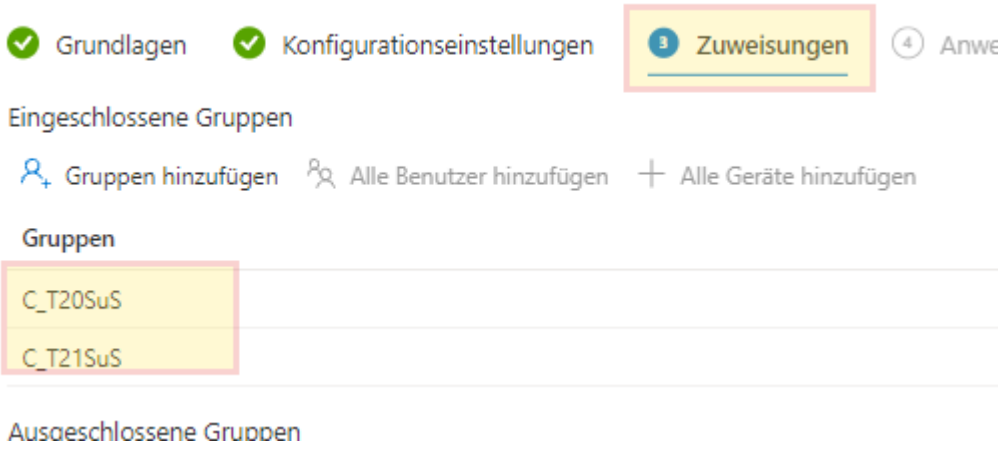
Name für das Profil frei wählbar – z.B.: „EDU-WORK“



WLan-Typ: Basis

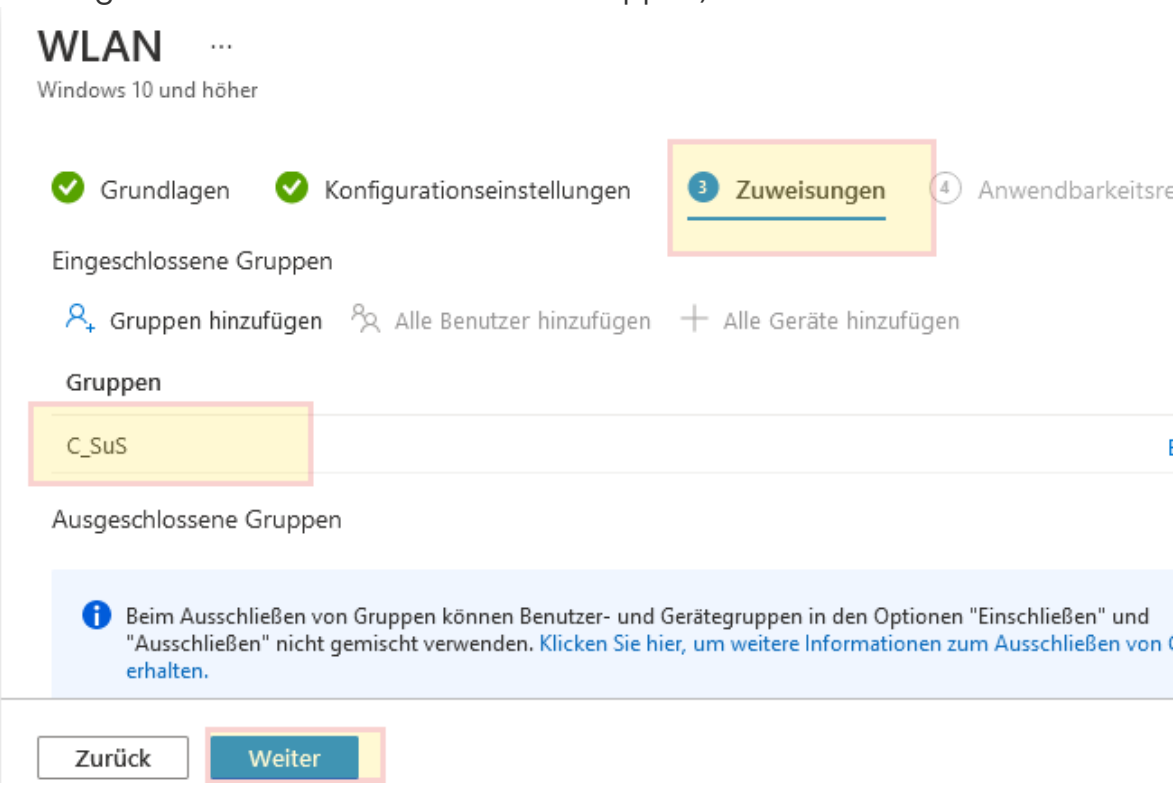


Zugewiesene Gruppen:
Wenn dieses WLan-Profil für alle Geräte aus der Geräteinitiative gelten soll, dann wählen wir die Gruppe „C_Autopilot“. Sollen beispielsweise für die Schüler und Lehrergeräte unterschiedliche WLan-Profile zugeordnet werden, dann die entsprechenden Gerätegruppen auswählen – wenn dieses WLan-Profil z. B. nur für die Schülergeräte gelten soll, dann sieht das so aus:

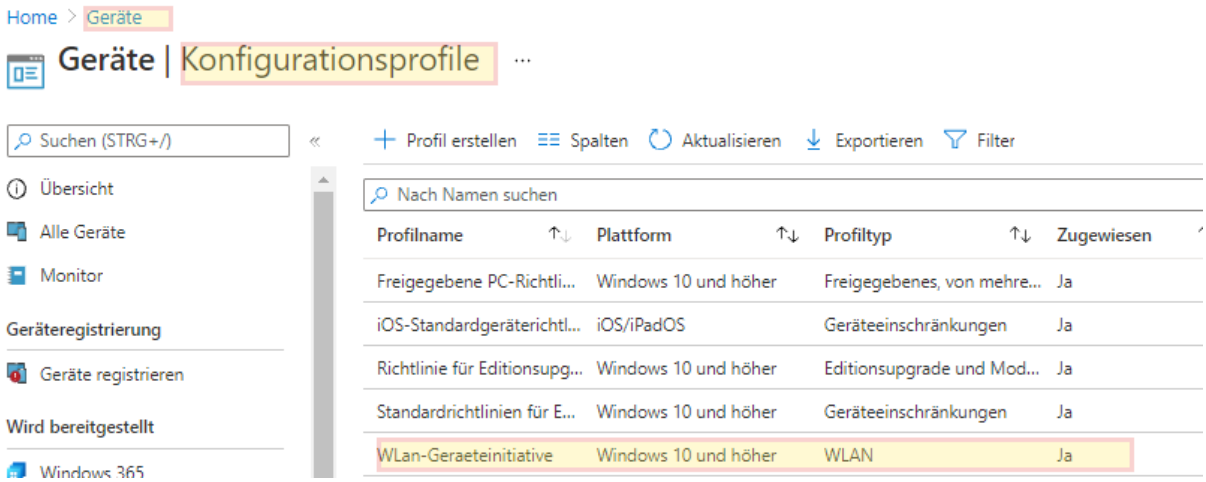


> Weiter > Weiter > Erstellen

Oder bei der Gruppenauswahl eine der statischen Gruppen (siehe Kap. 4.2 e) Erstellung von statischen LuL und SuS – Gruppen) verwenden:



Kontrolle:


Home > Geräte
Geräte | Konfigurationsprofile
Suchen (STRG+/)
Übersicht
Alle Geräte
Monitor
Geräteregistrierung
Geräte registrieren
Wird bereitgestellt
Windows 365
Profil erstellen
Spalten
Aktualisieren
Exportieren
Filter
Nach Namen suchen
Profilname
Plattform
Profiltyp
Zugewiesen
Freigegebene PC-Richtli... Windows 10 und höher Freigegebenes, von mehre... Ja
iOS-Standardgeräterichtl... iOS/iPadOS Geräteeinschränkungen Ja
Richtlinie für Editionsupg... Windows 10 und höher Editionsupgrade und Mod... Ja
Standardrichtlinien für E... Windows 10 und höher Geräteeinschränkungen Ja
WLan-Geraeteinitiative Windows 10 und höher WLAN Ja

Auswählen > Eigenschaften:

Grundlagen Bearbeiten

Name	EDU-Work
Beschreibung	WLAN für die Geräte aus der Gerät
Plattform	Windows 10 und höher
Profiltyp	WLAN

Konfigurationseinstellungen Bearbeiten

Verbindung mit bevorzugtem Netzwerk herstellen, sofern verfügbar	Ja
WLAN-Typ	Basis
WLAN-Name (SSID)	EDU-WORK
Verbindungsname	EDU-WORK
Automatisch verbinden, sofern in Reichweite	Ja
Verbindung mit diesem Netzwerk herstellen, auch wenn die SSID nicht übertragen wird	Ja
Limit für getaktete Verbindung	Uneingeschränkt
Sicherheitstyp für Drahtlosverbindung	WPA/WPA2-Persönlich
Vorinstallierter Schlüssel	******
FIPS-konformes (Federal Information Processing Standard) WLAN-Profil erzwingen	Nein
Proxyeinstellungen für Unternehmen	Keine

Bereichstags Bearbeiten

Standard

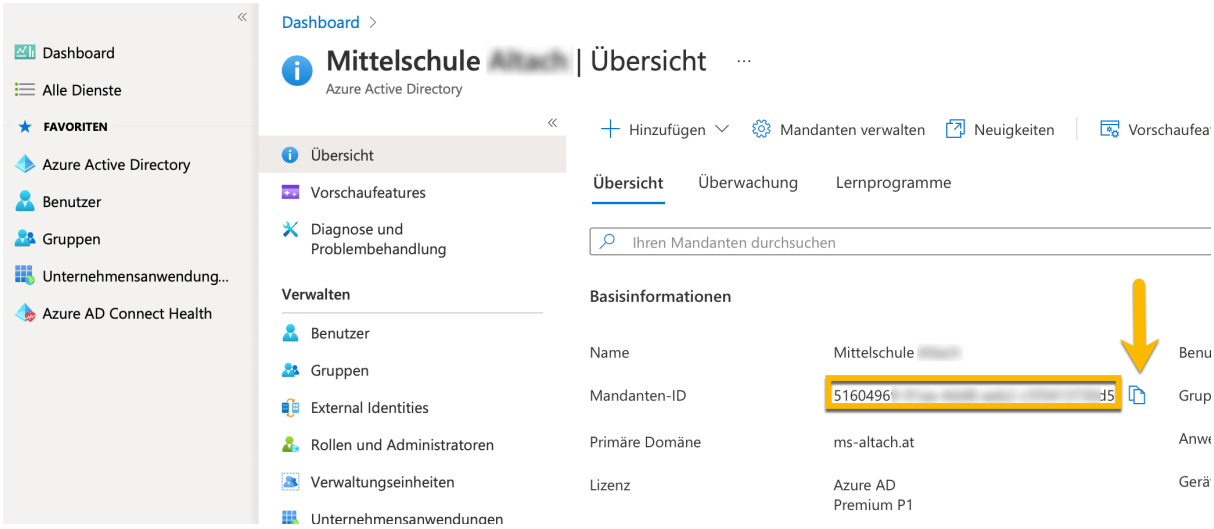
Zuweisungen Bearbeiten

Eingeschlossene Gruppen	C_T20SuS C_T21SuS
Ausgeschlossene Gruppen	--

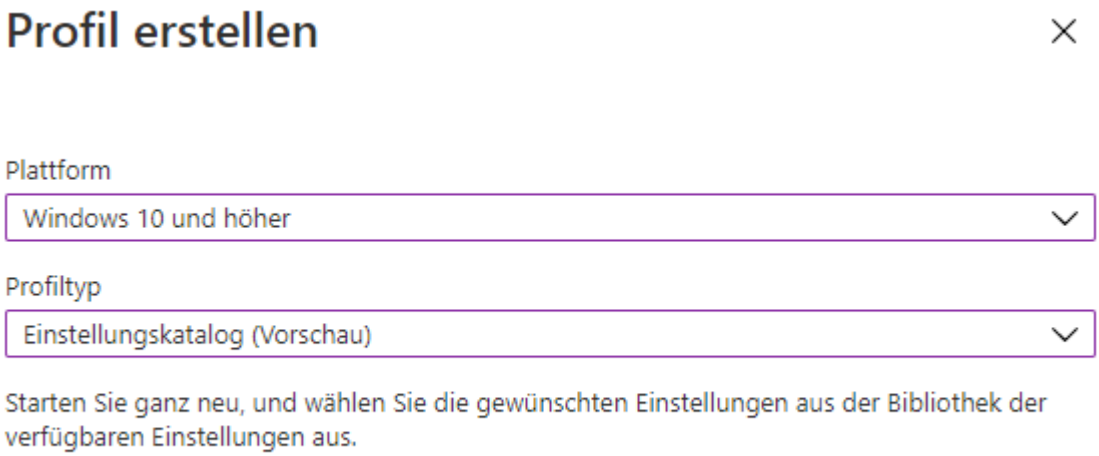
4.2.3 OneDrive automatisch bei der Anmeldung einbinden

Die Einrichtung dieser Richtlinie bewirkt, dass bei der Anmeldung mit den Azure AD – Zugangsdaten automatisch das OneDrive des Users eingerichtet und eingebunden wird.

Vorab muss im Azure Active Directory Admin Center in der Übersicht die Mandanten-ID ermittelt und (in der Zwischenablage) gespeichert werden.

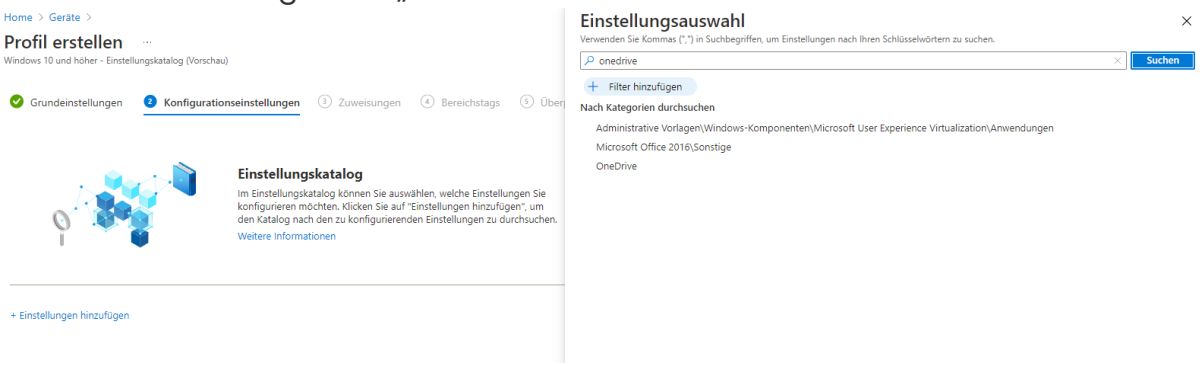


Im Microsoft Endpoint Manager Geräte – Konfigurationsprofile – „+ Profil erstellen“, „Windows 10 und höher“, „Einstellungskatalog (Vorschau)“:

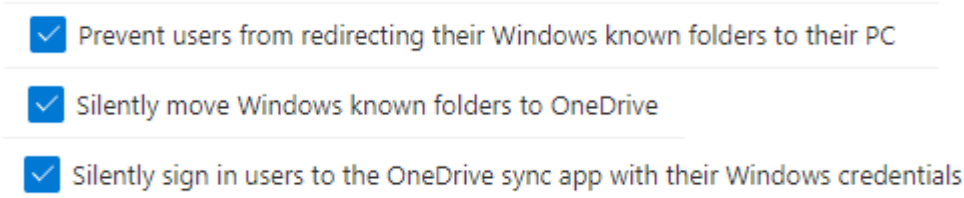


Wir nennen die Richtlinie „OneDrive einbinden“ und wählen dann bei den Konfigurationseinstellungen „+ Einstellungen hinzufügen“. Anschließend suchen

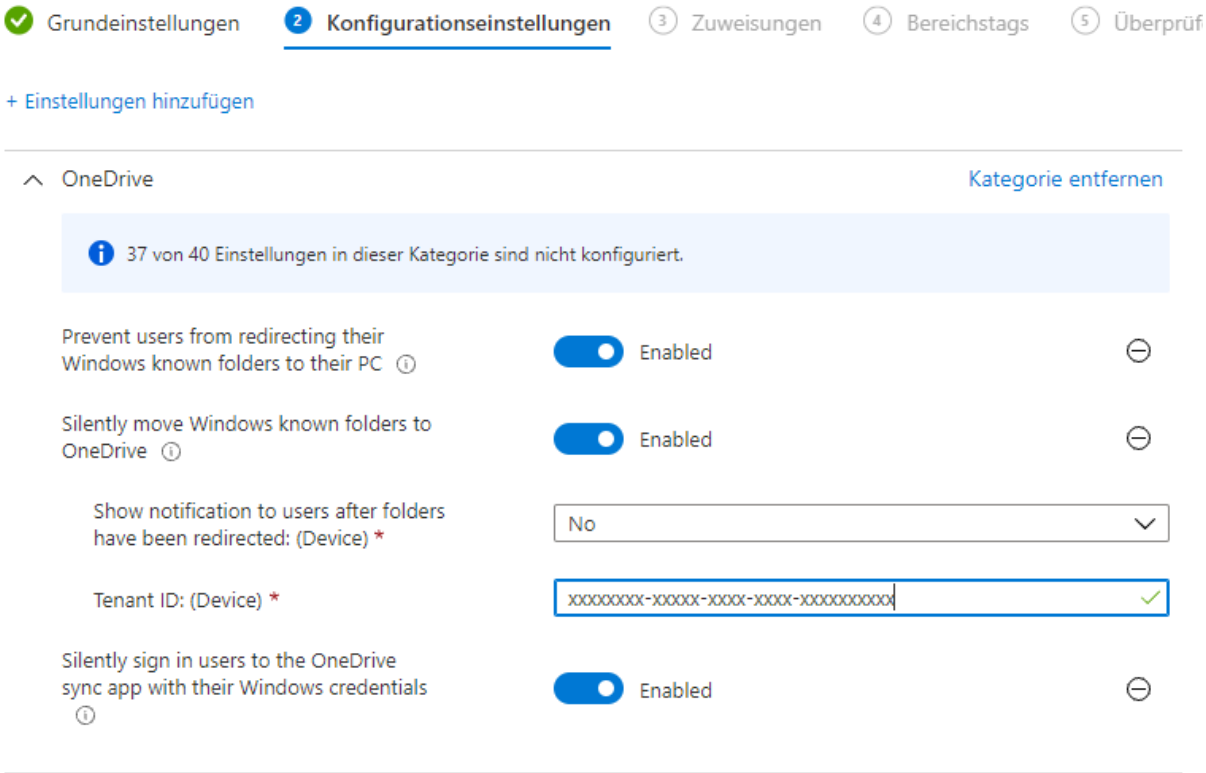
wir nach Einstellungen mit „OneDrive“:



Die Suche dauert etwas – nur Geduld.
Anschließend klicken wir „OneDrive“ an, und warten wieder. Im unteren Teil des Fensters werden jetzt alle OneDrive-Optionen angezeigt. Folgende davon aktivieren wir:



Im linken Teil des Fensters aktivieren wir dann diese gewählten Einstellungen und fügen die vorab kopierte Tenant ID (= Mandaten-ID) ein:



Abschließend weisen wir die Richtlinie den gewünschten Gruppen zu (Schülergruppen, Lehrergruppen oder alle), vergeben keine Bereichstags und stellen die Richtlinie dann fertig.

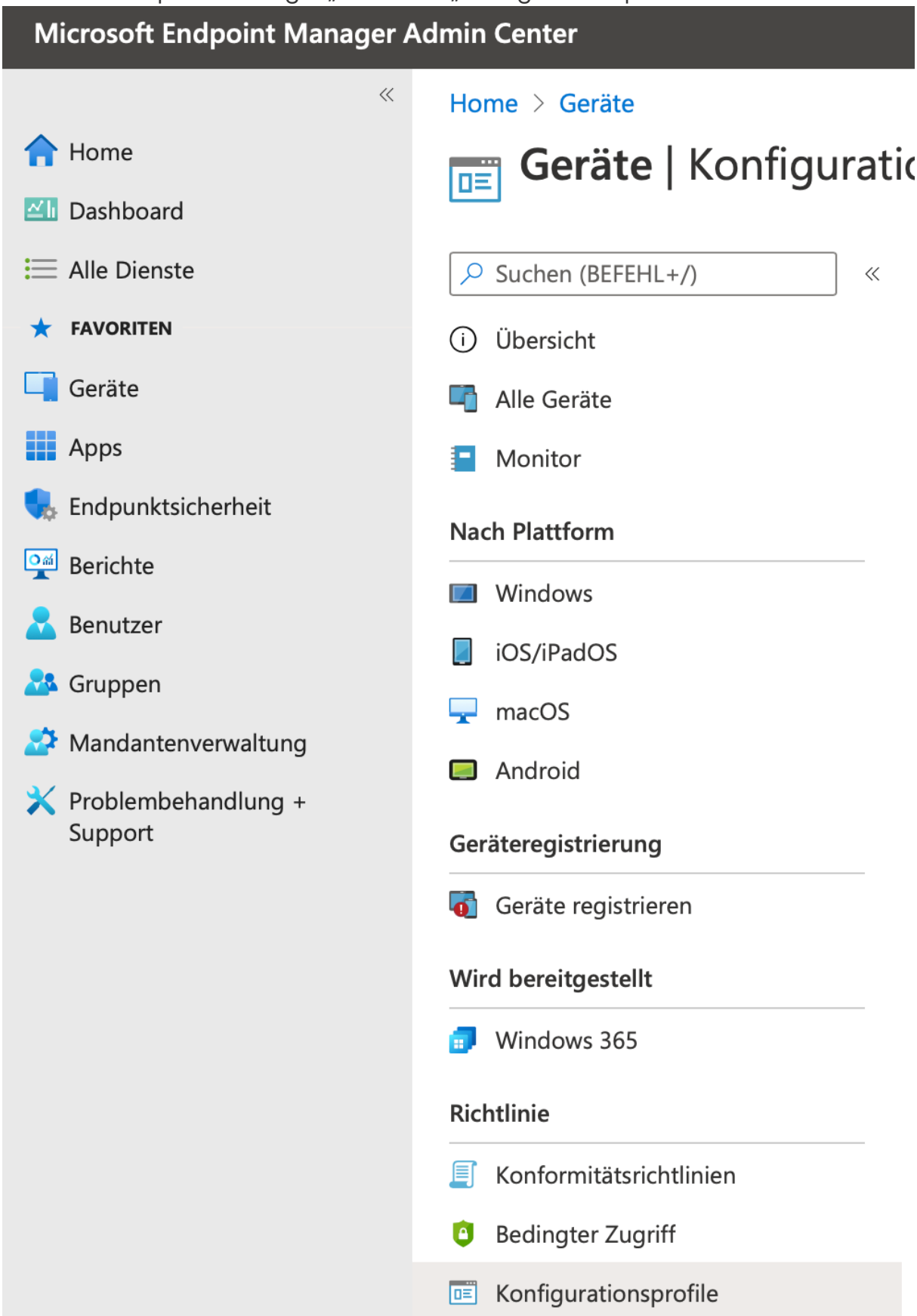
4.2.4 Standardanmeldedomäne einrichten

Während auf den lokalen PCs in der Schule nur der Benutzername eingegeben werden muss, ist es auf den per Microsoft Endpoint Manager verwalteten Geräten notwendig, dass auch die Domäne per @ angehängt wird.

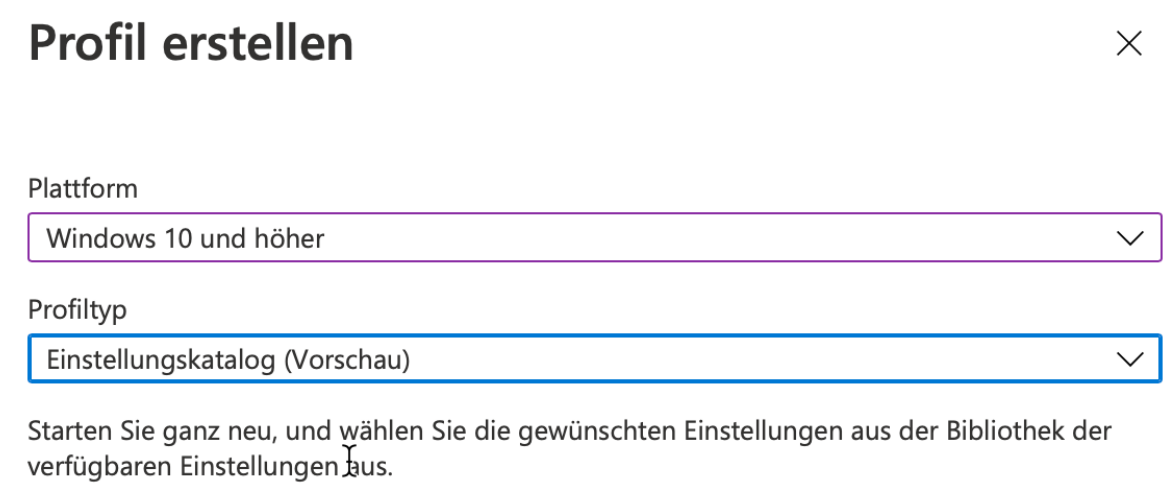
Da unsere Geräte aber sowieso nur im Kontext unserer Schule und mit unseren Usern verwendet werden sollen, können wir die Geräte so konfigurieren, dass die Schuldomäne als Voreinstellungen angenommen wird.

Dadurch können sich die Benutzer wie im lokalen Netzwerk mit dem Benutzernamen allein anmelden.

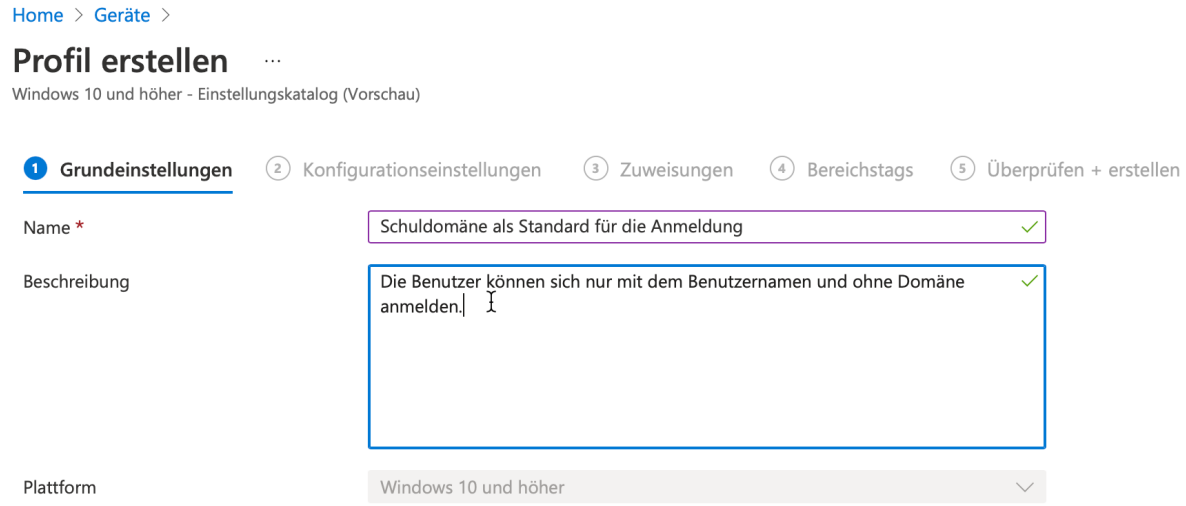
Microsoft Endpoint Manager „Geräte“ – „Konfigurationsprofile“ auswählen



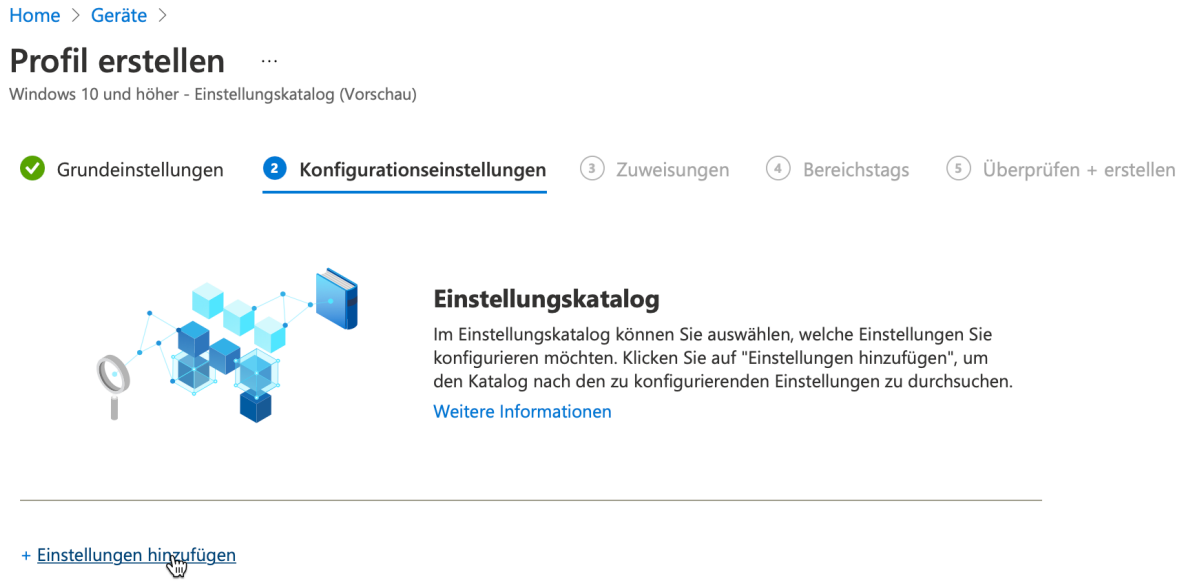
„+ Profil erstellen“ mit folgenden Einstellungen:



Einen sinnvollen nachvollziehbaren Namen verwenden „Schuldomäne als Standard für die Anmeldung“

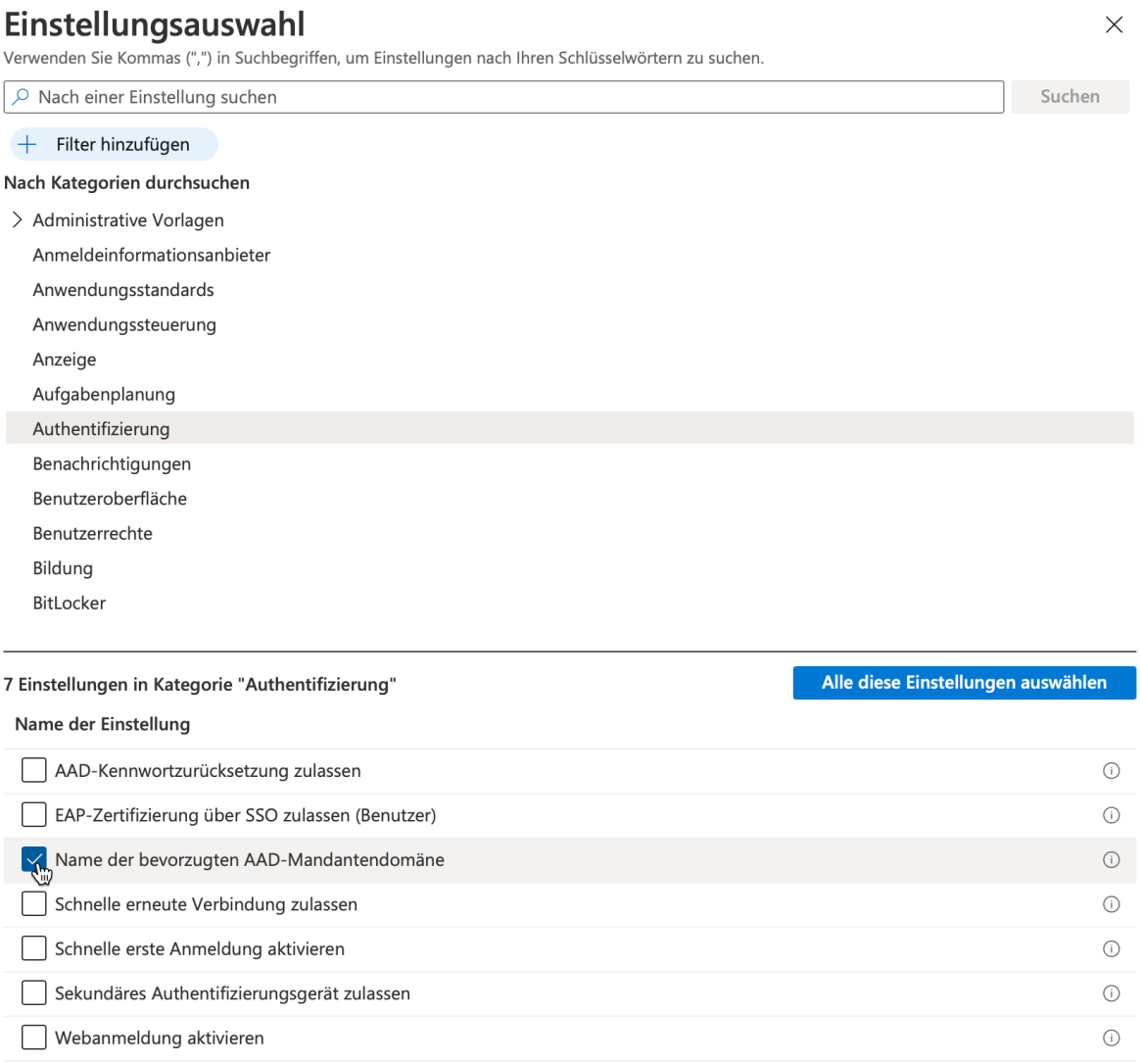


In den Konfigurationseinstellungen „+ Einstellungen hinzufügen“ auswählen

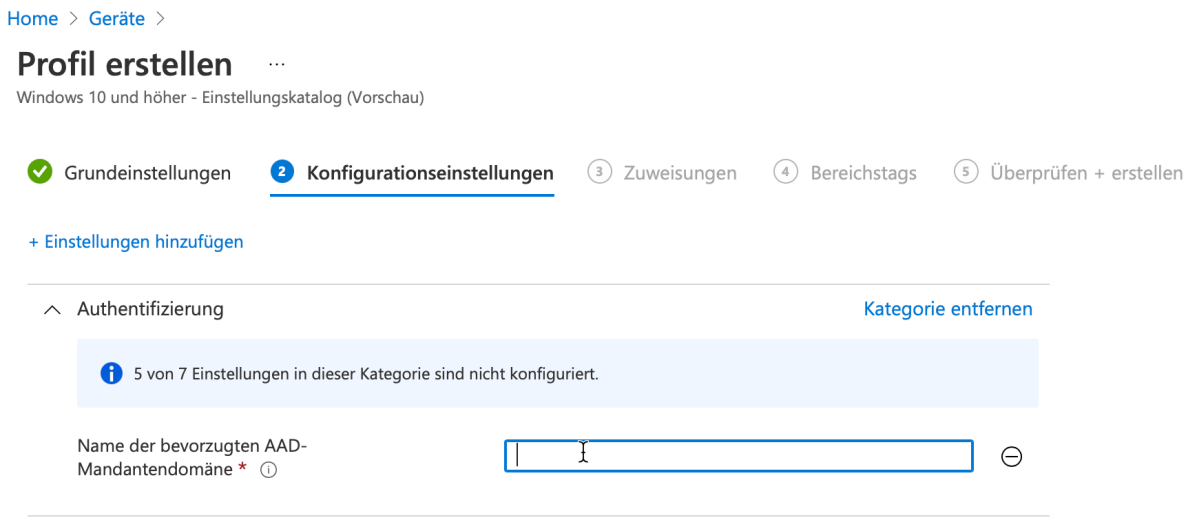


„Authentifizierung“ markieren (warten – es dauert ein paar Sekunden, bis die anderen Optionen angezeigt werden) und anschließend „Name der bevorzugten

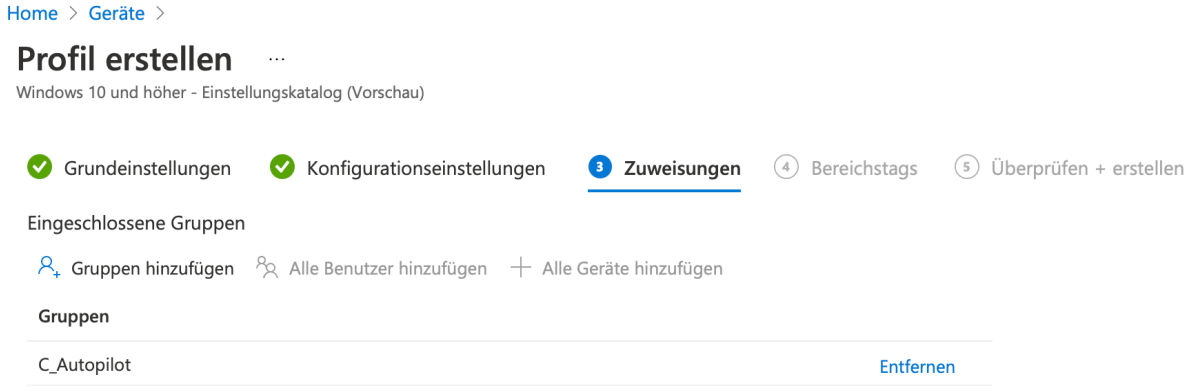
AAD-Mandantendomäne“ anklicken…



… und im linken Bereich die gewünschte Anmeldedomäne (ms-muster.at) der Schule eintragen:



Im nächsten Schritt weisen wir die Richtline der gewünschten Gerätegruppe (empfohlen C_Autopilot) zu.

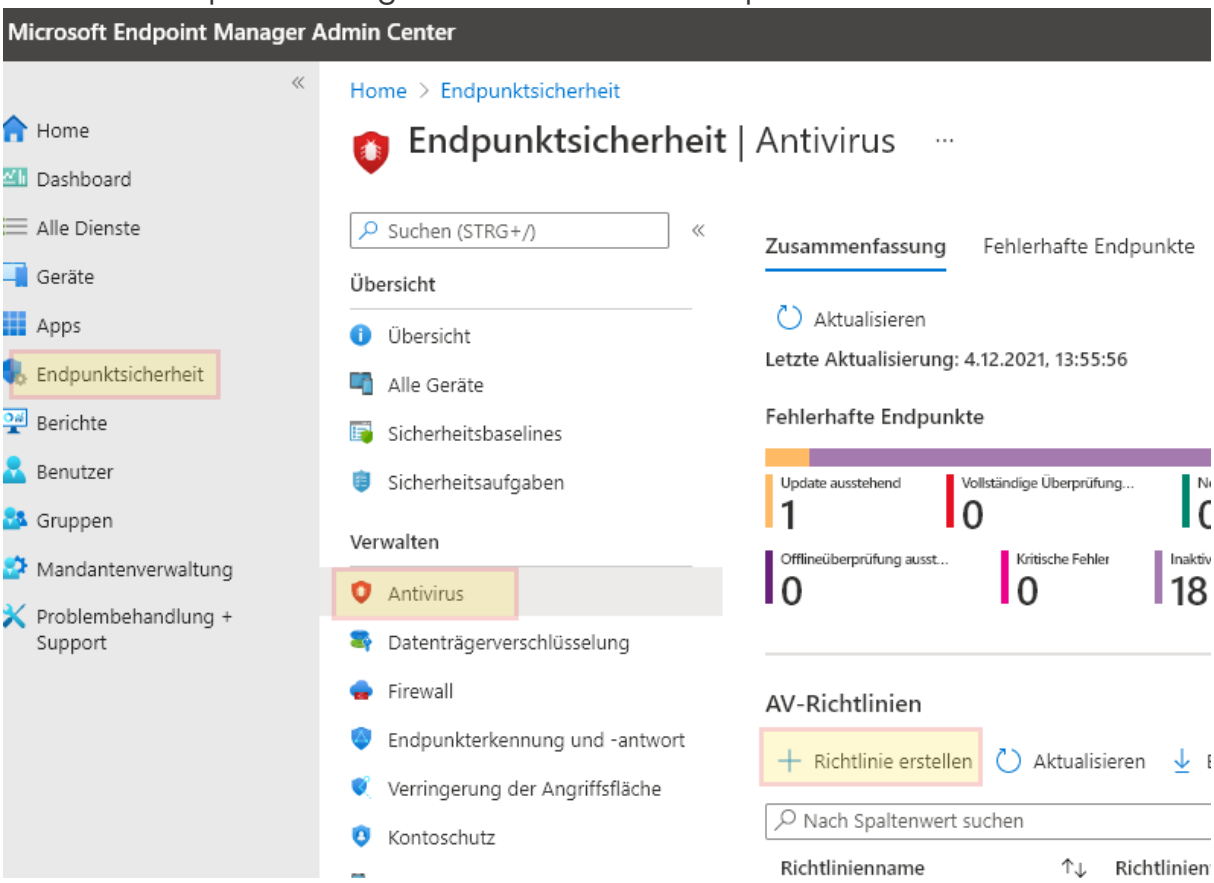


Diese Einstellung greift erst nach einem Neustart des Clients. Nach dem Neustart steht unter der Anmeldemaske nicht mehr „Anmelden an Firmen- oder Schulkonto“, sondern „Anmelden an: <Domänenname>“.

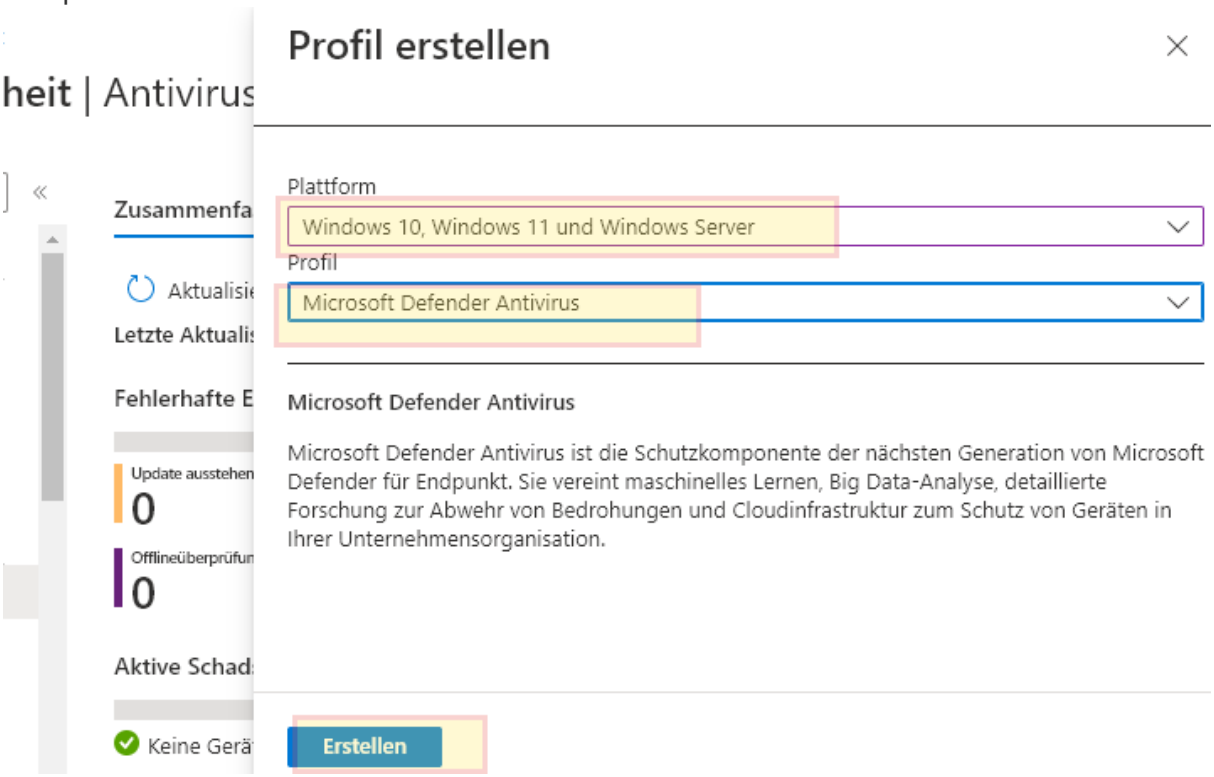
4.3 Antivirus – Voreinstellungen:

In der IKT-Schulverordnung wird ein “aktueller Schutz vor Schadsoftware auf digitalen Endgeräten zum Schutz des Schulnetzes” explizit gefordert. Die Einstellungen dazu:

Microsoft Endpoint Manager Admin Center -> Endpunktsicherheit:

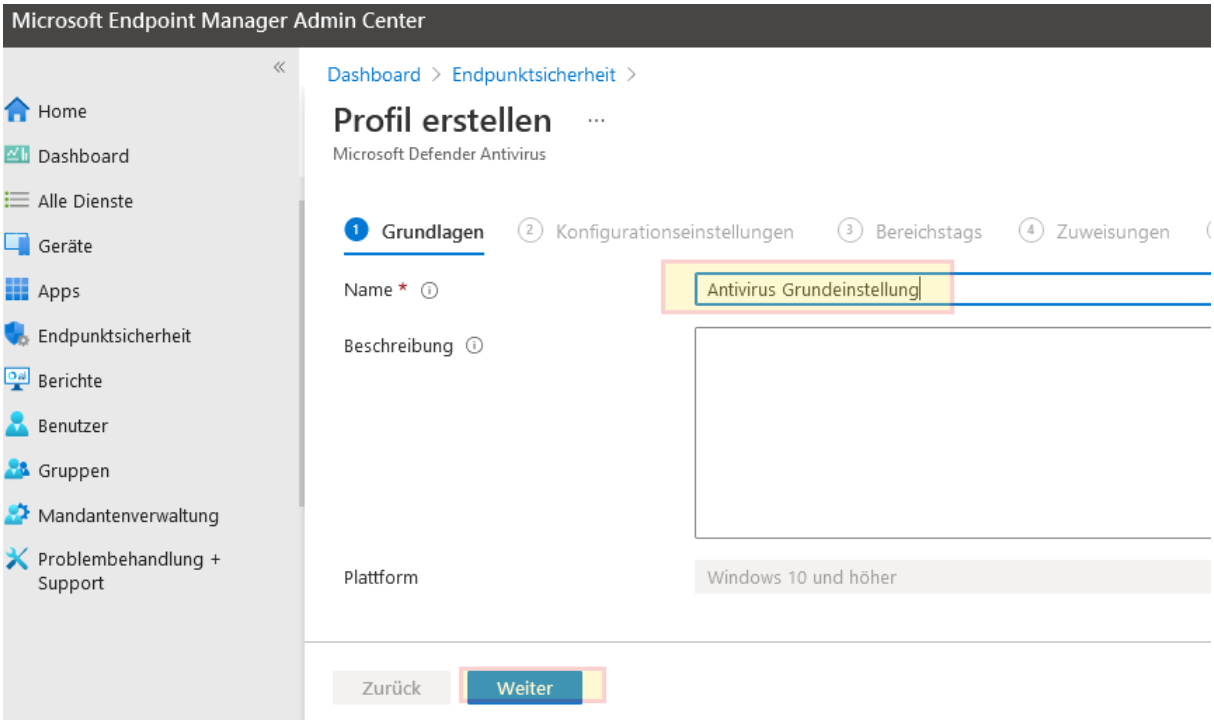


Endpunktsicherheit -> Antivirus -> Richtlinie erstellen

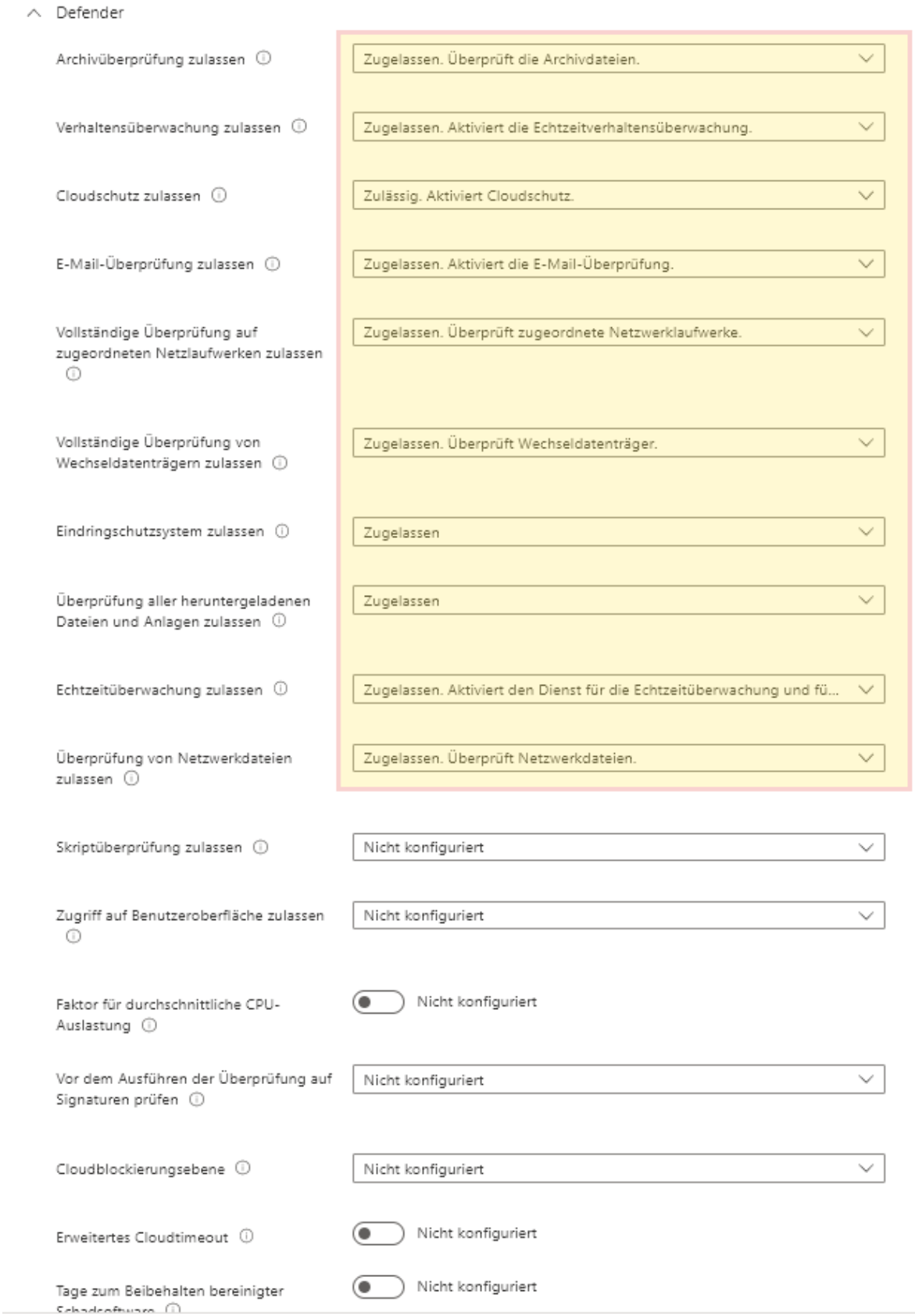


Plattform: Windows 10, Windows 11 und Windows Server
Profil: Microsoft Defender Antivirus

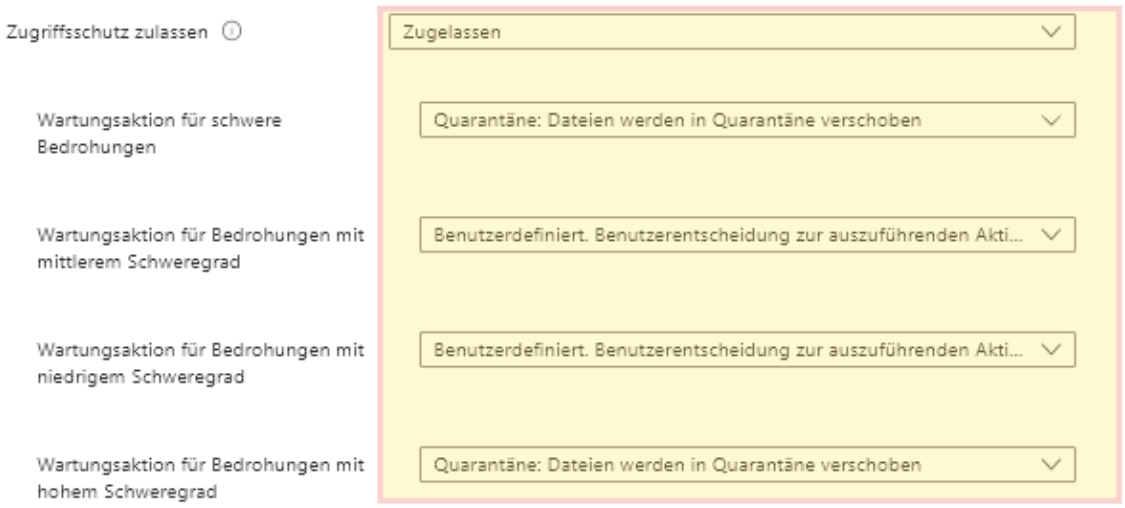
> Erstellen


Microsoft Endpoint Manager Admin Center
Home
Dashboard
Alle Dienste
Geräte
Apps
Endpunktsicherheit
Berichte
Benutzer
Gruppen
Mandantenverwaltung
Problembehandlung + Support
Dashboard > Endpunktsicherheit >
Profil erstellen
Microsoft Defender Antivirus
1 Grundlagen
2 Konfigurationseinstellungen
3 Bereichstags
4 Zuweisungen
Name *
Antivirus Grundeinstellung
Beschreibung
Plattform
Windows 10 und höher
Zurück
Weiter

Unter „Defender“ folgende Einstellungen vornehmen:



Vollständige Aufholüberprüfung deaktivieren	Nicht konfiguriert
Schnelle Aufholüberprüfung deaktivieren	Nicht konfiguriert
Niedrige CPU-Priorität aktivieren	Nicht konfiguriert
Netzwerkschutz aktivieren	Aktiviert (Überwachungsmodus)
Ausgeschlossene Erweiterungen	Nicht konfiguriert
Ausgeschlossene Pfade	Nicht konfiguriert
Ausgeschlossene Prozesse	Nicht konfiguriert
PUA-Schutz	Überwachungsmodus. Windows Defender erkennt potenziell unerwü...
Richtung für Echtzeitüberprüfung	Nicht konfiguriert
Überprüfungsparameter	Nicht konfiguriert
Schnellüberprüfungszeit planen	Nicht konfiguriert
Überprüfungstag planen	Nicht konfiguriert
Überprüfungszeit planen	Nicht konfiguriert
Fallbackreihenfolge für Signaturaktualisierung	Nicht konfiguriert
Dateifreigabequellen für Signaturaktualisierung	Nicht konfiguriert
Intervall für Signaturaktualisierung	Nicht konfiguriert
Zustimmung für das Senden von Stichproben	Nicht konfiguriert
Zusammenführung durch lokale Administratoren deaktivieren	Nicht konfiguriert

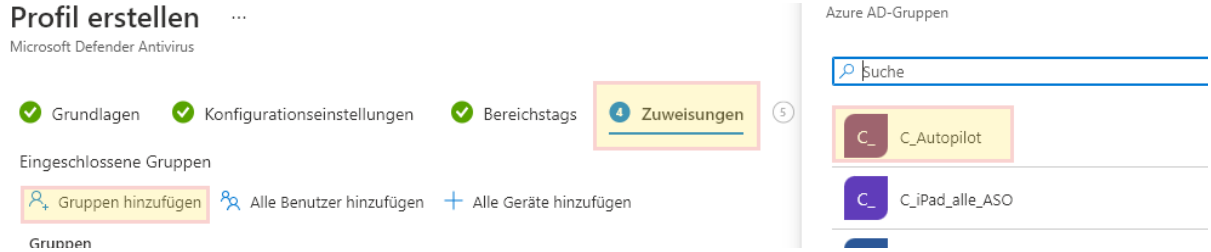


Optional können auch noch weitere Einstellungen in anderen Kategorien getroffen werden.

> ⚠ Zu restriktive Einstellungen führen dazu, dass z.B. die Powershell-Scripts, die wir über Intune zuweisen, auf den Geräten nicht mehr ausgeführt werden.

Wir werden hier weiter testen (Stand 27.09.22), welche zusätzlichen Einstellungen möglich bzw. sinnvoll sind (und die Scripts auf den Clients trotzdem laufen) und diese Anleitung entsprechend aktualisieren.

kein Bereichstag -> weiter
Zuweisungen: “Eingeschlossene Gruppen”: Entweder den Punkt “Alle Geräte hinzufügen” wählen oder unsere Gerätegruppe “C-Autopilot” hinzufügen:



> “auswählen” > “Weiter” > “Erstellen”

5 Lokales Administratorkonto für Lehrergeräte

Da die Lehrergeräte nicht in den Privatbesitz übergehen, richten wir zusätzlich einen lokalen Administrator ein, damit jederzeit ein Vollzugriff auf das Lehrergerät für den IT-Betreuer, MDM-Betreuer oder dgl. gewährleistet ist.

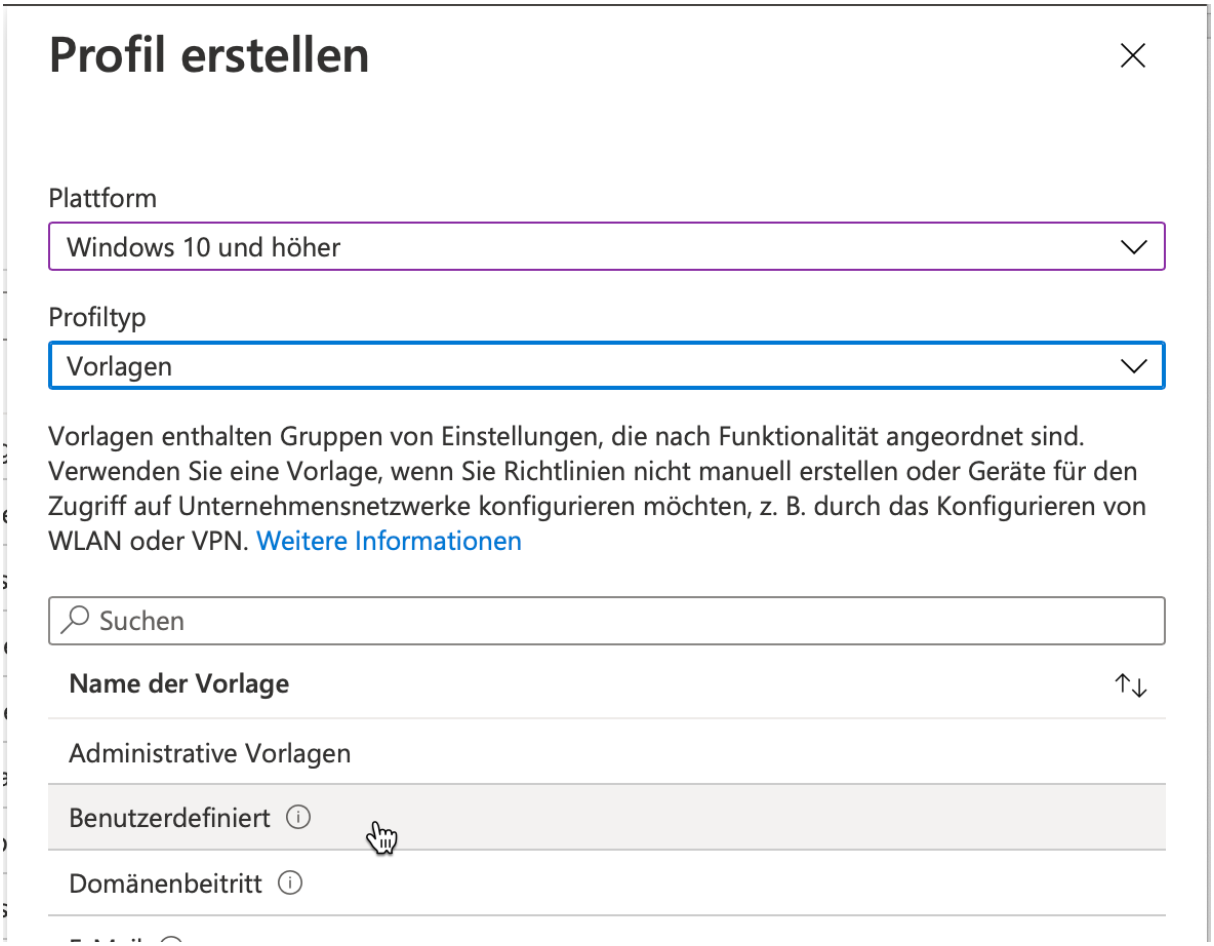
Grundsätzlich ist bei aktiver Registrierung und Internetanbindung ein Login auf dem Gerät als MS365-Admin auch möglich, um damit lokale Adminrechte auf dem Gerät zu bekommen. Sollte aber etwas mit der Registrierung oder der Internetanbindung nicht funktioniert, ist es hilfreich, sich lokal als Administrator anmelden zu können.

Da der vorab eingerichtete lokale Administrator über den MS Endpoint Manager nicht verwaltet werden kann, erstellen wir einen eigenen Admin-User.

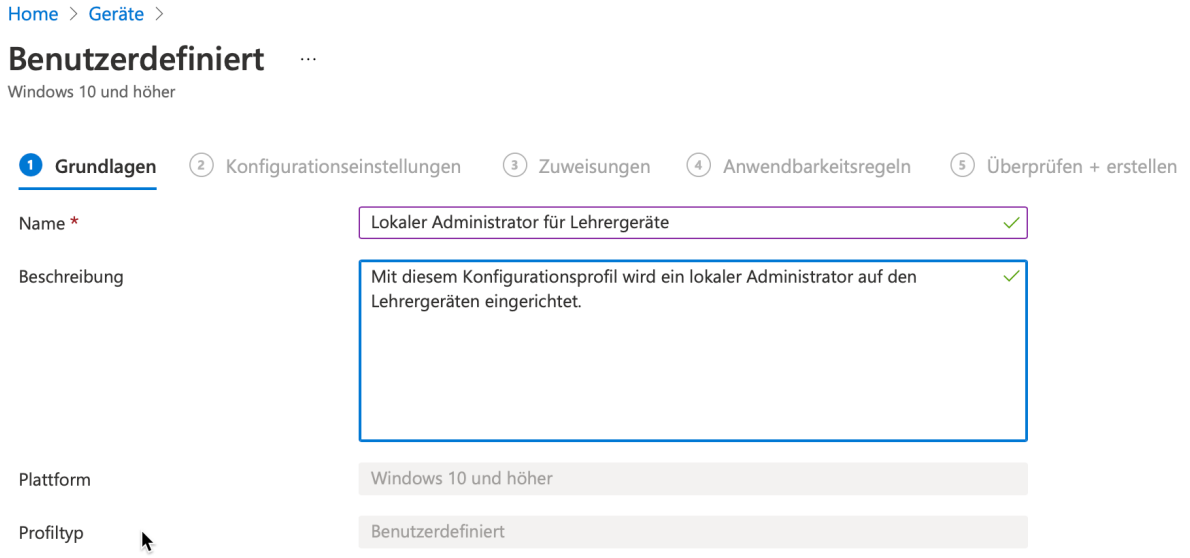
Natürlich wäre es möglich, über ein Skript (entweder Batch oder Powershell) den lokalen Administrator mit einem Kennwort zu versehen. Allerdings werden alle Skripts in einem lokal gespeicherten Logfile im Klartext gespeichert und können von jedem User ausgelesen werden – daher der Umweg über einen eigenen Admin-User.

Im Endpoint Manager Admin Center auf Geräte – Konfigurationsprofile wechseln und ein neues Profil erstellen:

„Windows 10 und höher“, „Vorlagen“ und bei den Vorlagen „Benutzerdefiniert“ auswählen – anschließend auf „Erstellen“.



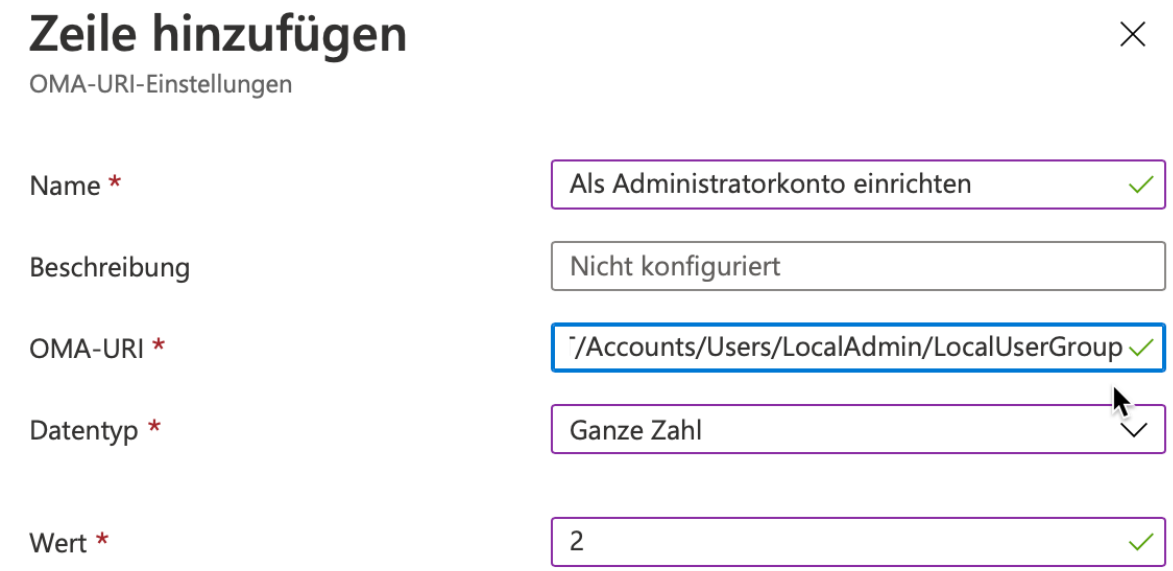
Mit nachvollziehbarem Namen und entsprechender Beschreibung versehen:



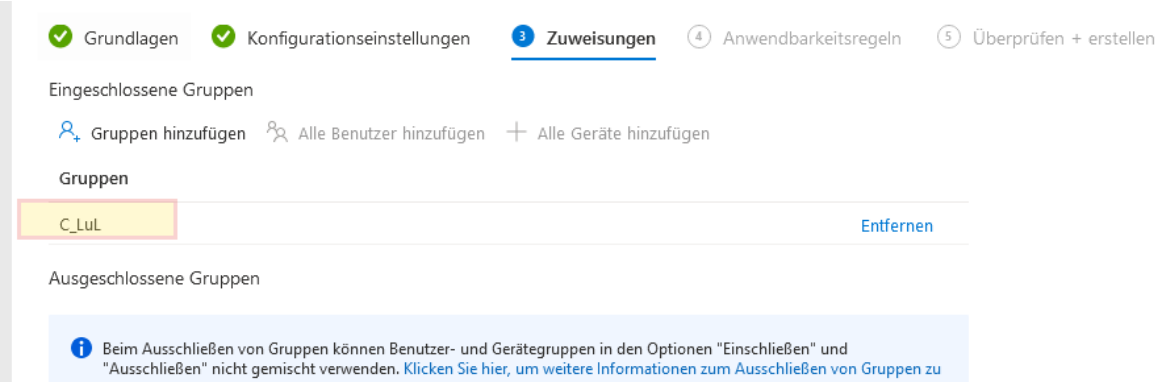
Bei OMA-URI-Einstellungen folgende zwei Einträge hinzufügen (LocalAdmin ist in diesem Fall der gewünschte Benutzername des neuen Adminkontos):
Name: Lokales Administratorkonto
Beschreibung: <kann leer bleiben>
OMA-URI: ./Device/Vendor/MSFT/Accounts/Users/LocalAdmin/Password
Datentyp: Zeichenfolge
Wert: <das gewünschte Kennwort>

Zweiter Eintrag (mit diesem wird das Konto als Mitglied der Administratorengruppe eingerichtet):

Name: Als Administratorkonto einrichten
Beschreibung: <kann leer bleiben>
OMA-URI: ./Device/Vendor/MSFT/Accounts/Users/LocalAdmin/LocalUserGroup
Datentyp: Ganze Zahl
Wert: 2



Bei den Zuweisungen nun noch der Gruppe C_T21LuL (bzw. C_N21LuL) oder der statischen Gruppe „C_LuL“ zuweisen.



Die Anwendbarkeitsregeln bleiben leer.
Sobald die Regel erstellt ist, wird sie an die Lehrergeräte ausgeliefert.

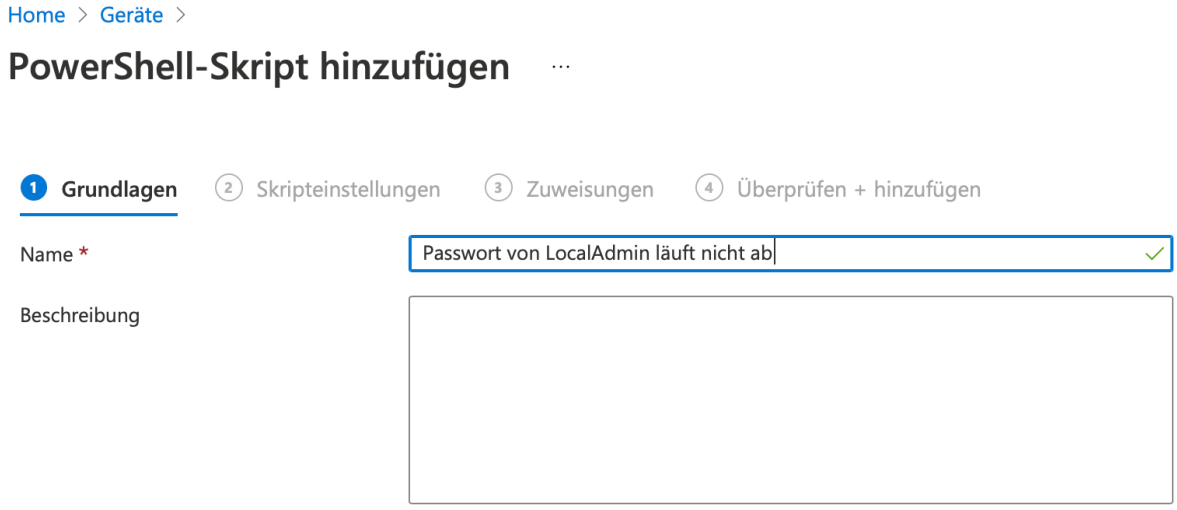
Weiters müssen wir noch ein Skript erstellen und anwenden lassen, damit die Gültigkeit des Passworts nicht abläuft.
Das Skript ist ein Einzeiler:

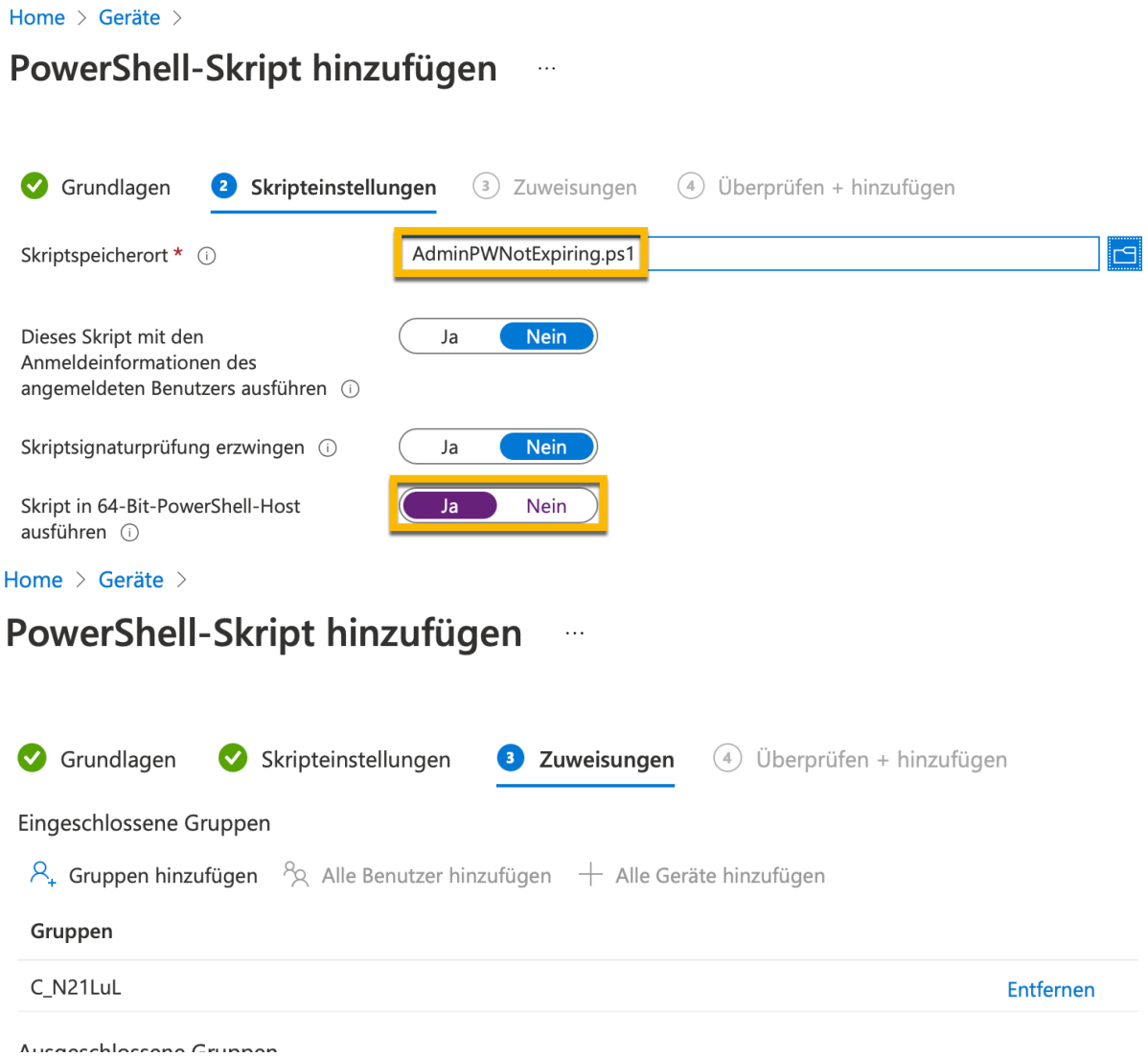
```
wmic USERACCOUNT WHERE "Name='LocalAdmin'" SET PasswordExpires=FALSE
```

Downloadmöglichkeit:
https://www.vobs.at/fileadmin/user_upload/itservice/downloads/digitaleendgeraete/AdminPWNotExpiring.ps1.zip

Dieses Skript muss als ps1-Datei abgespeichert werden (z.B. AdminPWNotExpiring.ps1) und unter Geräte – Skripts hinzugefügt werden (inkl. „Skript in 64-Bit-Powershell-Host ausführen"!)

Endpoint Manager: „Geräte" – „Skripts" - „+Hinzufügen" – „Windows 10"





Von der eventuellen Fehlermeldung „-2016281112 (Remedation failed)“, die in der Übersicht bei dieser Konfiguration angezeigt wird, darf man sich dabei nicht irritieren lassen – es funktioniert dennoch.

Die Anmeldung auf dem Client erfolgt über den Anmeldenamen „.\LocalAdmin“ oder „localhost\LocalAdmin“ (anstelle von „.“ bzw. „localhost“ kann auch der Gerätename verwendet werden) und dem gewählten Kennwort.

6 Windows-Autopilot-Registrierung

6.1 CSV-Datei für den Import erstellen:

Der Übersicht zuliebe kopieren wir die versch. Hardware-Hashes in eine Exceldatei.

Zwingend sind die drei Spalten:

- Device Serial Number
- Windows Product ID (bleibt bei uns leer)
- Hardware Hash

Wir verwenden zusätzlich diese Spalten (das ist wichtig, sonst funktionieren weder die dynamischen Gruppen noch das ganze damit verknüpfte Konzept):

- Group Tag
- Assigned User

Zum Importieren können wir eine gemeinsame Liste für die SuS- und LuL-Geräte verwenden.

	A	B	C	D	E
1	Device Serial Number	Windows Product ID	Hardware Hash	Group Tag	Assigned User
2	5CG6052CRW		T0FiBAEAHAAAAAoAPAJhSg	T21LuL	anton.lehrer@msegg.at
3	5CG6052RVD		T0FgAwEAHAAAAAoAPAJhS	T20SUS	21.fritz.schueler@msegg.at

Damit daraus eine CSV-Datei mit dem richtigen Format, dem richtigen Trennzeichen (=Beistrich) und dem richtigen Zeichensatz wird, müssen wir aus Excel einen Export machen und dann die resultierenden CSV-Dateien mit dem Editor (Notepad) final bearbeiten

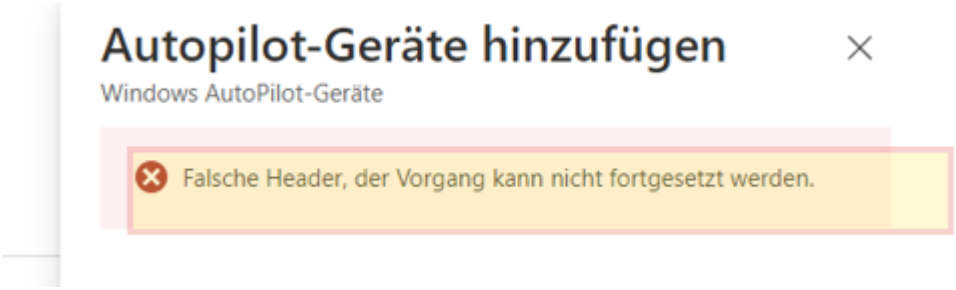
- vorab die fertige Exceldatei im normalen Excelformat noch einmal speichern
- Excel – speichern unter „CSV (Trennzeichen getrennt) (*.csv)“
- Datei mit normalen Windows-Editor (Notepad) öffnen
  - Strichpunkte durch Beistriche ersetzen
  - neu abspeichern als – bei Codierung: „UTF-16 LE“

> Excel „merkt“ sich alle Zellen, in denen irgendwann einmal ein Wert (Zahl oder Text) enthalten war. Solange man in Excel arbeitet, merkt bzw. sieht man davon nichts – beim Export bzw. „speichern unter“ als CSV-Datei werden diese irgendwann einmal befüllt gewesenen Zellen aber ebenfalls mit exportiert.

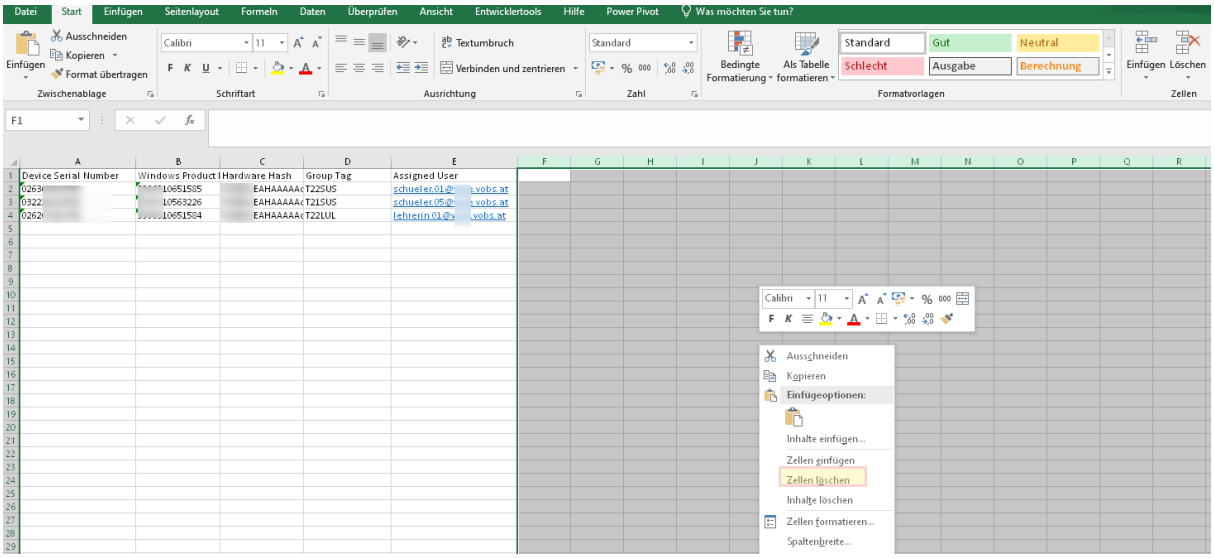
Die Folge ist eine CSV-Datei die zu viele Spalten oder Zeilen enthält. Ersichtlich ist das aber erst, wenn die CSV-Datei mit dem Editor geöffnet wird. Hier sind dann hinten in bei jedem Datensatz zusätzliche Trennzeichen (Strichpunkte bzw.

Beistriche) enthalten – siehe:

Intune quittiert in so einem Fall den Autopilot-Geräteimport per csv-Datei mit dem Fehler:



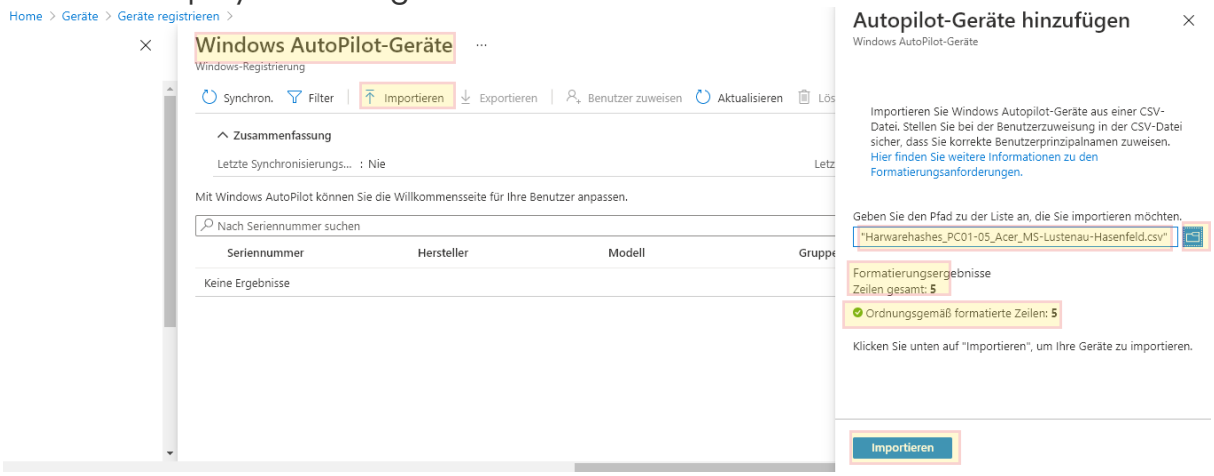
Abhilfe:
In Excel zusätzlich befüllte Zellen (Spalten und/oder Zeilen) nicht nur „inhaltlich“ löschen, sondern die ganzen Spalten/Zeilen markieren und diese dann löschen. Am besten zur Sicherheit vor dem csv-Export einige der leeren Spalten rechts markieren und mit RK „Zellen löschen“ komplett löschen (dasselbe auch mit einigen der leeren Zeilen unterhalb der befüllten Zeilen):



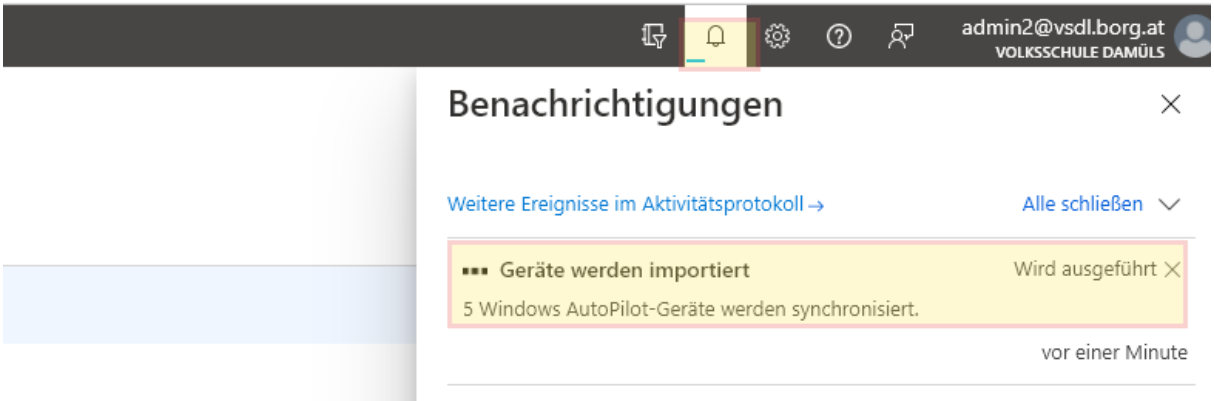
Excelmappe speichern und erst dann den Export machen.

6.2 CSV-Dateien in Intune importieren:

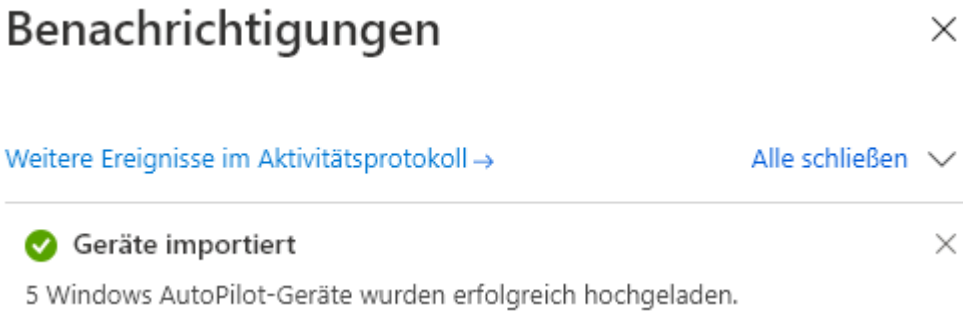
Geräte > Geräte registrieren > Windows-Registrierung > unter „Windows AutoPilot Deployment-Programm“: Geräte



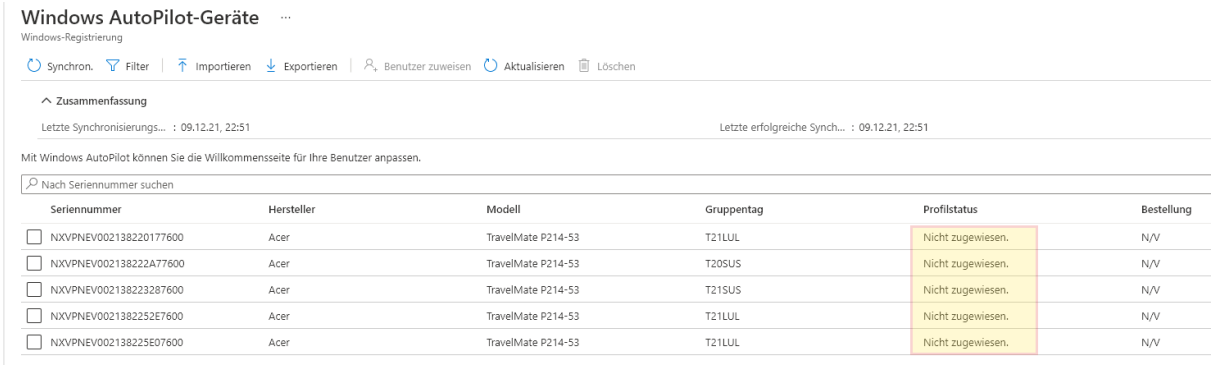
Das kann dauern – ganz oben bei den Benachrichtigungen sieht man, dass etwas im Gange ist:



… nach 3 min:

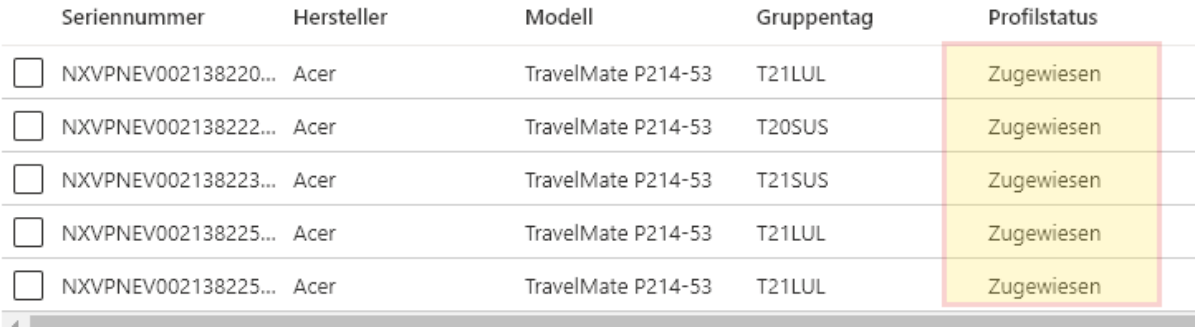


Vorerst lautet der Profilstatus „Nicht zugewiesen“:

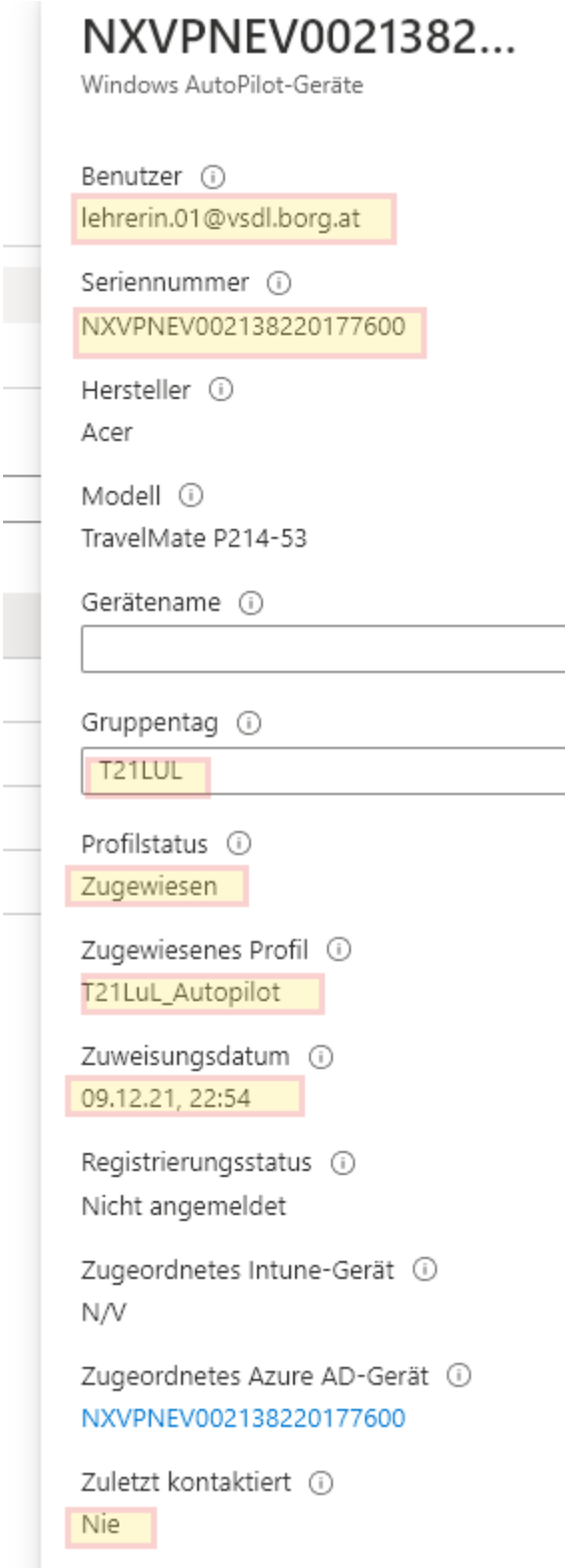


Nach weiteren vier Minuten wechselt der Profilstatus auf „Wird aktualisiert“:

Das ist aber immer noch nicht der Zustand, den wir benötigen – bitte warten, bis bei Profilstatus „Zugewiesen“ steht – nach weiteren 4 min ist es so weit:



Klickt man auf eines der registrierten Geräte, so werden rechts die Details dieser Autopilot-Registrierung angezeigt:



- Der Benutzer ist zugeordnet; das Gerät ist über die Seriennummer registriert (auch im Azure-AD); das PC-Modell (TravelMate P214-53) wurde automatisch erkannt; der Gruppentag ist ersichtlich; Profilstatus ist „zugewiesen“; das zugewiesene Autopilot-Profil lautet „T21LuL_Autopilot“

- Der Gerätename kommt dann erst mit der tatsächlichen Verbindung des Gerätes mit dem Internet und er anschließenden Konfiguration (bis dato haben wir am Gerät noch nichts gemacht).
- Zu diesem Zeitpunkt steht hier die Seriennummer des Gerätes als Gerätename im „Azure-AD“. Der richtige Computername wird erst nach dem Rollout (= Gerät starten, anmelden ...) erstellt und zugeordnet.
- Das Gerät hat sich bis jetzt noch nicht mit Intune verbunden (passt – wir haben es ja noch gar nicht gestartet).

Weitere Infos zum Generieren der Hardware-Hashes von bereits vorhandenen Geräten:
https://docs.microsoft.com/de-de/mem/autopilot/add-devices

6.2.1 Überprüfen der dynamischen Zuweisung

Die per Autopilot angemeldeten Geräte starten nur dann wie gewünscht, wenn das Geräteprofil auch erfolgreich zugewiesen wurde. In wenigen Fällen kann diese Zuweisung auch länger dauern – erfahrungsgemäß bis zu zwei Stunden.

Nach dem Import der CSV-Dateien kann dies überprüft werden.

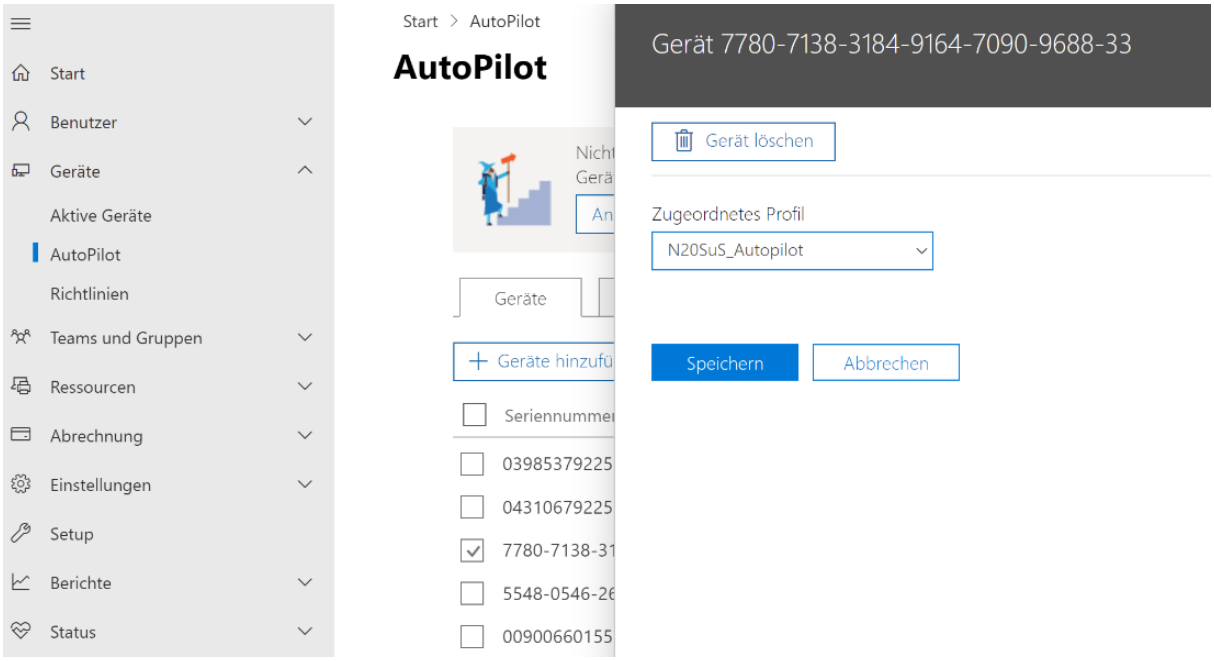
Azure Active Directory > Geräte > Alle Geräte > Gerät auswählen

Wenn die Gruppe C_Autopilot und C_T21xxx bzw. C_N21xxx auftaucht (die Zuordnung wird durch die dynamische Richtlinie durchgeführt), so greift in weiterer Folge auch das entsprechende Geräteprofil bei der Anmeldung.

Scheint die Gruppe hier noch nicht auf, so wurde die dynamische Zuordnung noch nicht durchgeführt.

Das Geräteprofil für die Einrichtung der Computer kann auch manuell zugeordnet werden:

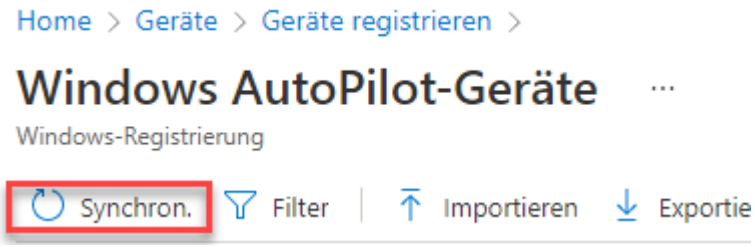
Microsoft 365 admin center > Geräte > Autopilot > Gerät auswählen und Profil zuordnen



Ein manuell zugewiesenes Profil wird in weiterer Folge durch eine dynamische Zuordnung überschrieben, sobald diese durch den Endpoint Manager ausgewertet wird. Es ist nicht möglich, dauerhaft anderes ein Autopilot-Profil zuzuordnen!

Nach der manuellen Zuordnung muss diese mit dem Microsoft Endpoint Manager noch synchronisiert werden (wobei auch das nach einiger Zeit automatisch durchgeführt wird):

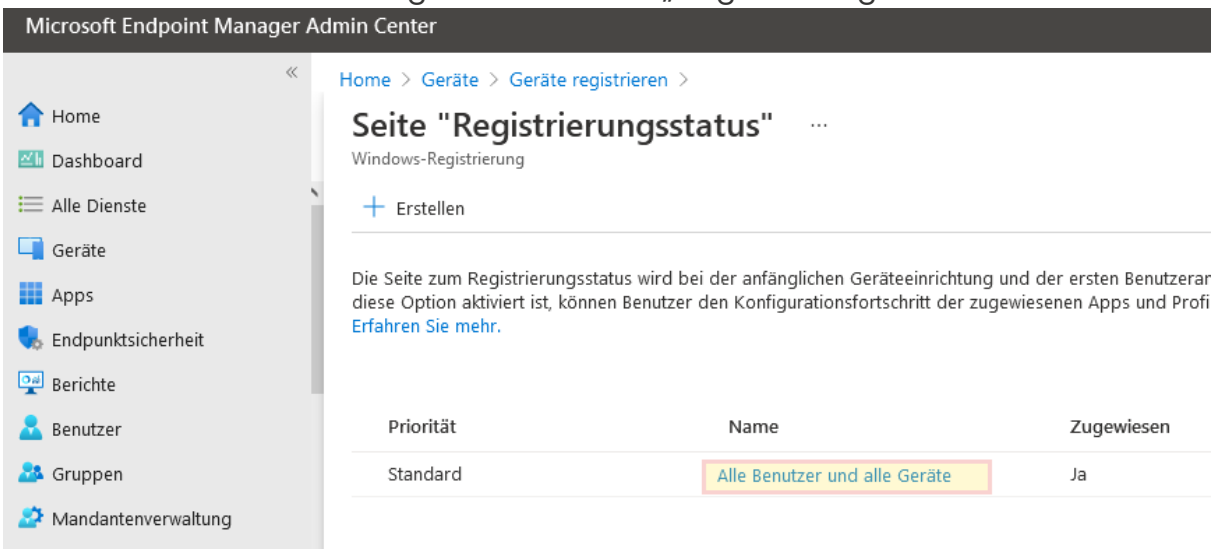
Endpoint Manager > Geräte > Geräte registrieren > Geräte und Synchron.



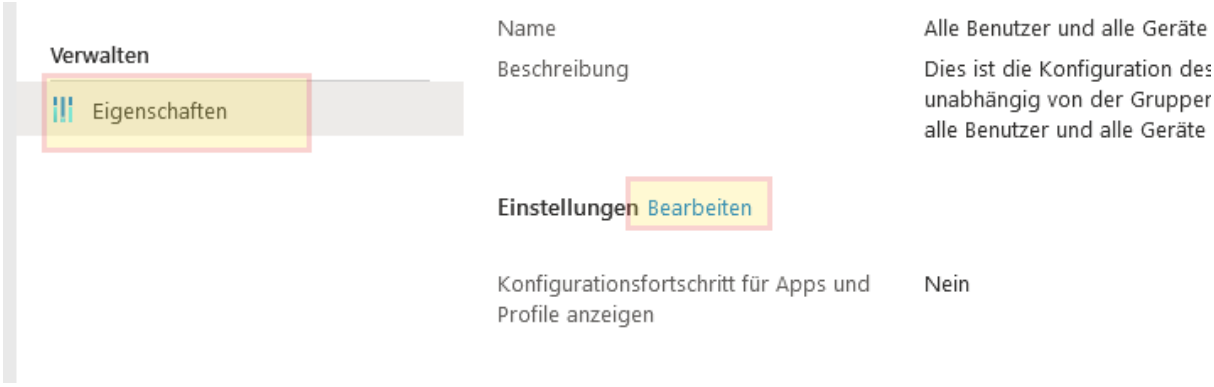
6.3 Seite: Registrierungsstatus

Wir aktivieren die Seite zum Registrierungsstatus. Damit wird auf den Clients der Bereitstellungsfortschritt angezeigt, wenn ein neues Gerät registriert wird. Die Benutzer sehen den Konfigurationsfortschritt der Registrierung, der Profile und der zugewiesenen Apps auf ihrem Gerät.

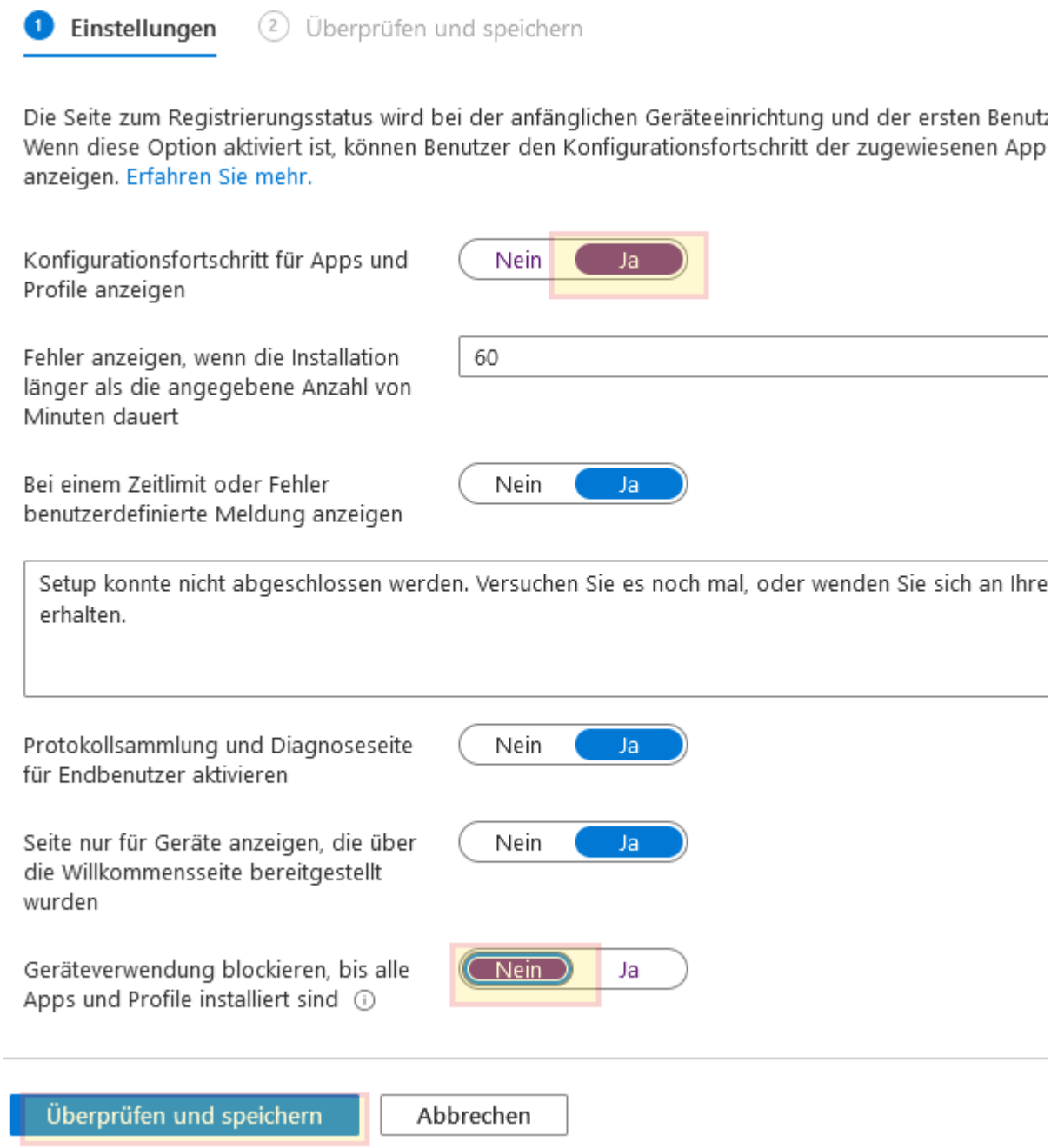
Intune > Geräte > Geräte registrieren > Seite „Registrierungsstatus“:



Eigenschaften – Einstellungen bearbeiten:



Einstellungen:



6.4 Rollout: Geräte erstmals starten:

Ist diese Zuweisung vollständig:
= alle Geräte vorhanden und bei allen steht bei Profilstatus „Zugewiesen“
… können die Geräte erstmalig gestartet werden.

7 Apps- und Softwareverteilung

> ⚠ Wir empfehlen, die Softwareverteilung nicht parallel mit der Erstkonfiguration (Registrierung …) durchzuführen.

Grund: eventuelle Überlastung des Netzwerkes (Internet). Praxiserfahrungen dazu mit vielen synchronen Registrierungen fehlen uns leider. Wenn der (einmalig durchzuführende) Registrierungsprozess fehlschlägt (z. B. „timeout“ wegen Netzwerküberlastung), muss das jeweilige Geräte u. U. zurückgesetzt werden und das kann dauern.

Den Registrierungsprozess also abwarten und erst anschließend die Softwareverteilung „scharf“ stellen: Die jeweils abschließende Zuweisung zu den Gerätegruppen (z.B. „C-Autopilot“) somit erst nach dem erfolgreichen Registrierungsprozess durchführen.

Sind die Programme einmal auf den Geräten installiert, kann bei den jeweiligen Apps die Gerätegruppenzuordnung wieder rausgenommen werden - die bereits installierten Apps und Programme bleiben auf den Geräten erhalten.

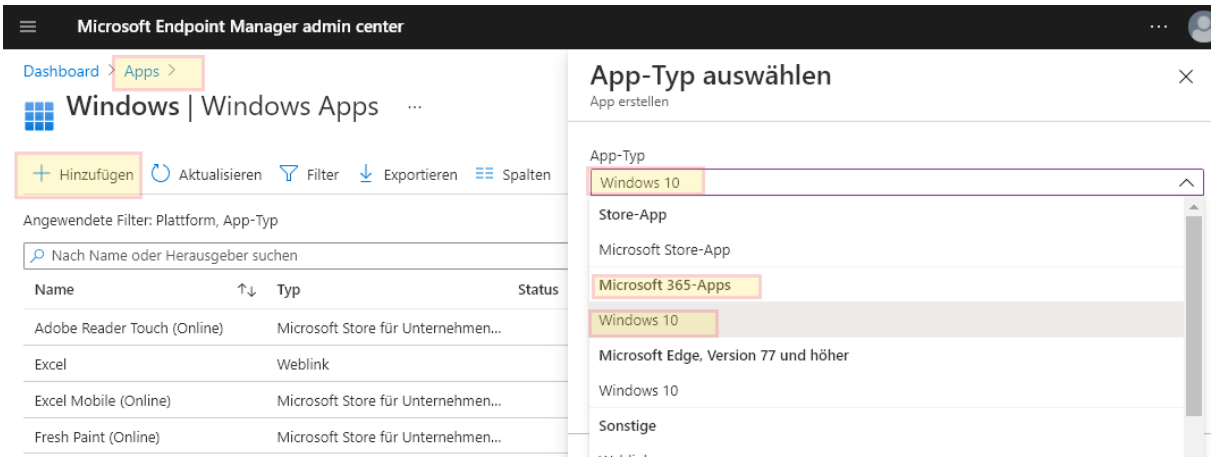
Vor einer weiteren Registrierungsaktion mit einer ganzen Klasse würden wir aus derzeitiger Sicht diese Vorgangsweise empfehlen: Also vor der „Rollout-Stunde“ die Gerätegruppenzuordnung (z.B. zu „C-Autopilot“) bei den Apps und Progs rausnehmen und erst nach Abschluss des Registrierungsprozesses wieder implementieren.

7.1 Office-Suite:

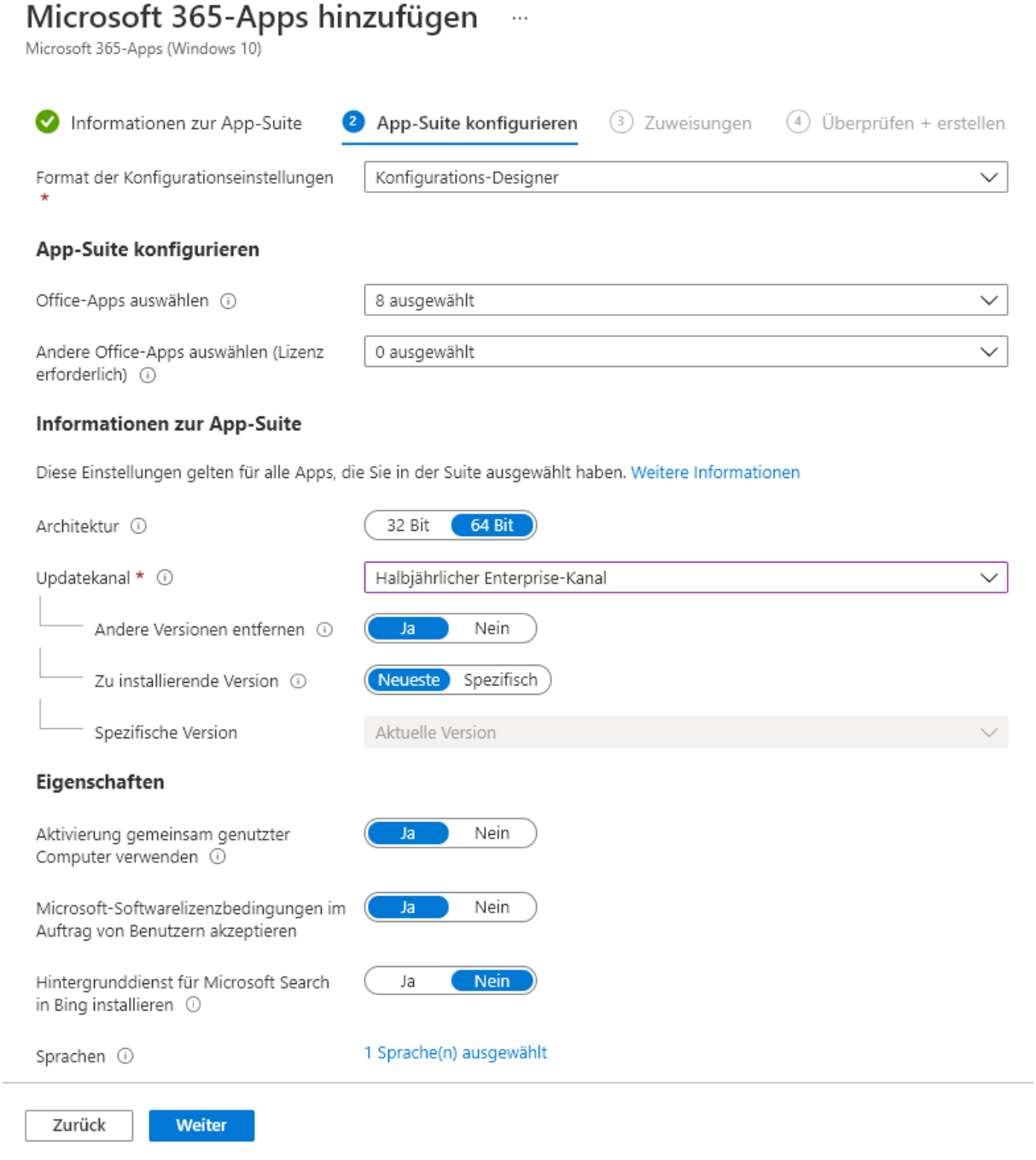
Das Office Pro Plus – Programmpaket heißt jetzt nur noch „Microsoft 365-Apps für Windows 10“ bzw. nur noch „Microsoft 365 Apps“. Die Office Suite kann direkt über Intune den Geräten zugeordnet werden. Es braucht dazu weder einen Vorab-Einkauf im Store noch die Bereitstellung eines MSI-Paketes.

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

Apps > Windows > Hinzufügen > bei App-Typ unter der Kategorie „Microsoft 365-Apps“ „Windows 10“ auswählen:

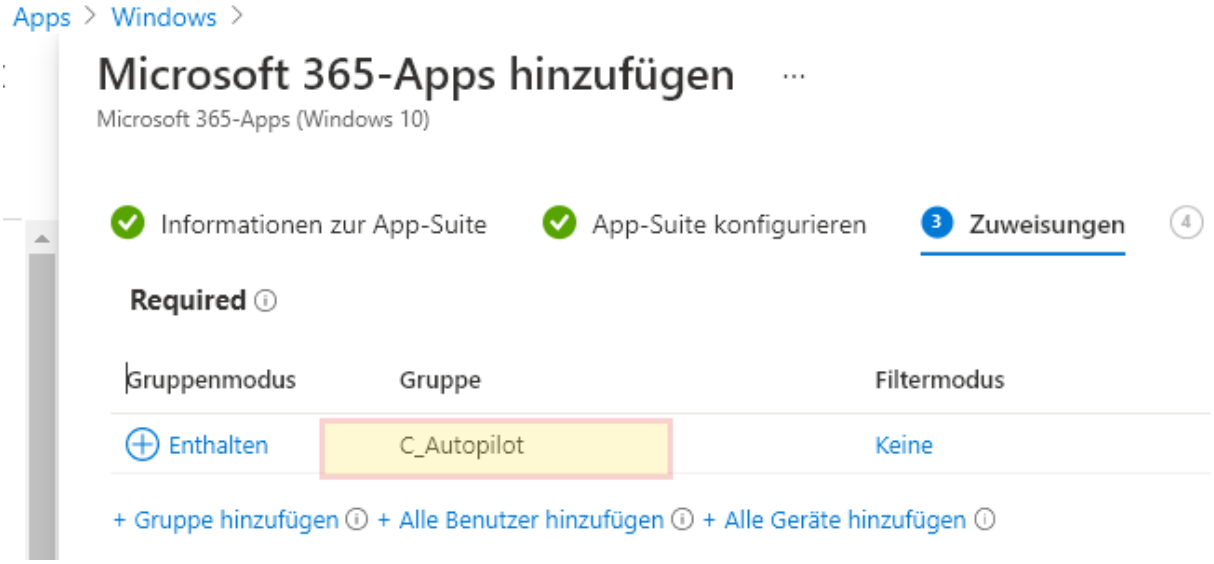


Bei „Informationen zur App-Suite“ „weiter“ > App-Suite konfigurieren



Wichtig: Gewünschte Zielsprache auswählen

Zuweisungen:
Im Normalfall wird die Office-Suite auf allen Geräten erforderlich sein. Deshalb wählen wir als Gerätegruppe „C-Autopilot“ bei „Required“ (= Programm wird auf allen Geräten der ausgewählten Gruppe(n) automatisch installiert)



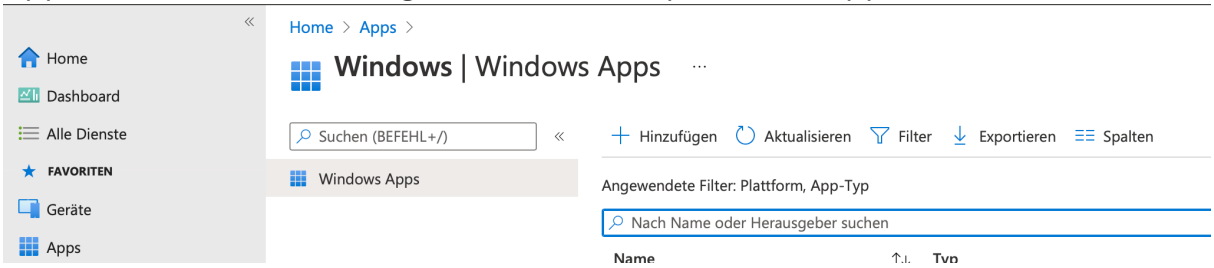
> Erstellen

7.2 MSI-Pakete

Leider funktionieren nicht alle MSI-Pakete (z.B. nicht alle vom VOBS für die Softwareverteilung über die Gruppenrichtlinien zur Verfügung gestellten) über diese Installationsvariante.

In solchen Fällen muss nach funktionierenden msi-Paketen Ausschau gehalten werden oder eine der zusätzlichen Verteilungsmöglichkeiten in Intune verwendet werden.

Apps – Windows – hinzufügen – „Branchenspezifische App“ auswählen



App-Typ auswählen

App erstellen

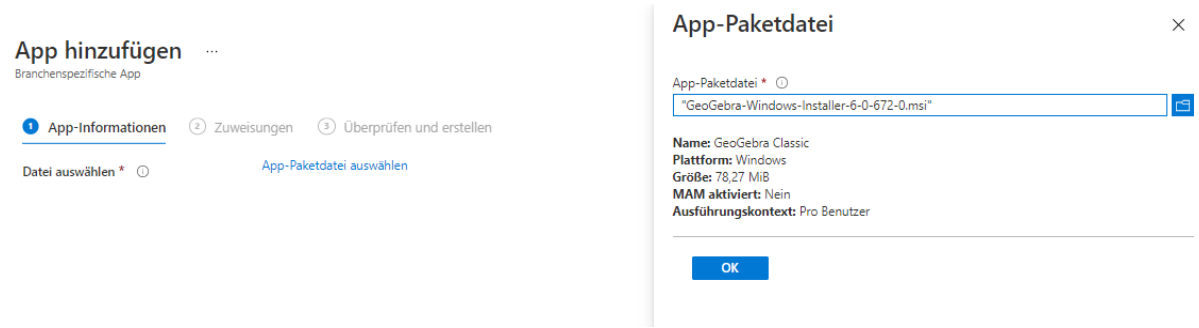
App-Typ

Branchenspezifische App

Branchenspezifische App

Um eine benutzerdefinierte oder interne App hinzuzufügen, laden Sie die Installationsdatei der App hoch. Stellen Sie sicher, dass die Erweiterung mit der vorgesehenen Plattform der App übereinstimmt. Intune unterstützt die folgenden Plattformen und Erweiterungen für branchenspezifische Apps:

- Android (APK)
- iOS (IPA)
- macOS (.IntuneMac)
- Windows (.msi, .appx, .appxbundle, .msix und .msixbundle)



App hinzufügen ...

Branchenspezifische Windows MSI-App

1 App-Informationen 2 Zuweisungen 3 Überprüfen und erstellen

Datei auswählen * GeoGebra-Windows-Installer-6-0-672-0.msi

Name * GeoGebra Classic

Beschreibung * GeoGebra Classic

Beschreibung bearbeiten

Herausgeber * Geogebra

App-Installationskontext Benutzer Gerät

App-Version ignorieren Ja Nein

Befehlszeilenargumente

Kategorie 0 ausgewählt

Diese App als ausgewählte App im Unternehmensportal anzeigen Ja Nein

Informations-URL Geben Sie eine gültige URL ein.

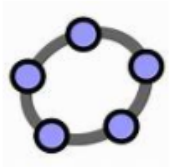
URL zu den Datenschutzbestimmungen Geben Sie eine gültige URL ein.

Entwickler

Besitzer

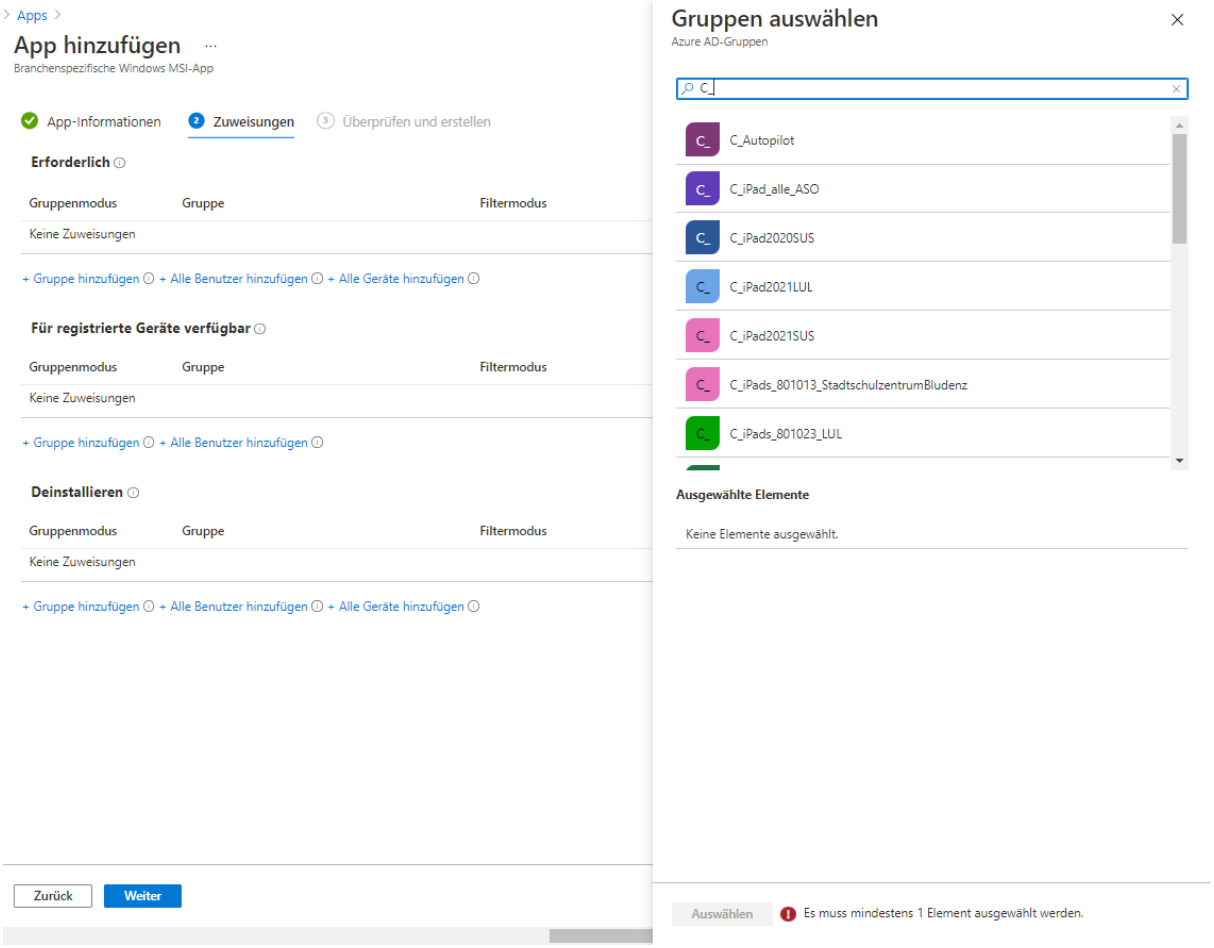
Hinweise

Logo Bild ändern



Zurück Weiter

App Paketdatei auswählen > MSI-Paket auswählen > Herausgeber und evtl. Logo einfügen > erforderliche Gruppe zuweisen.

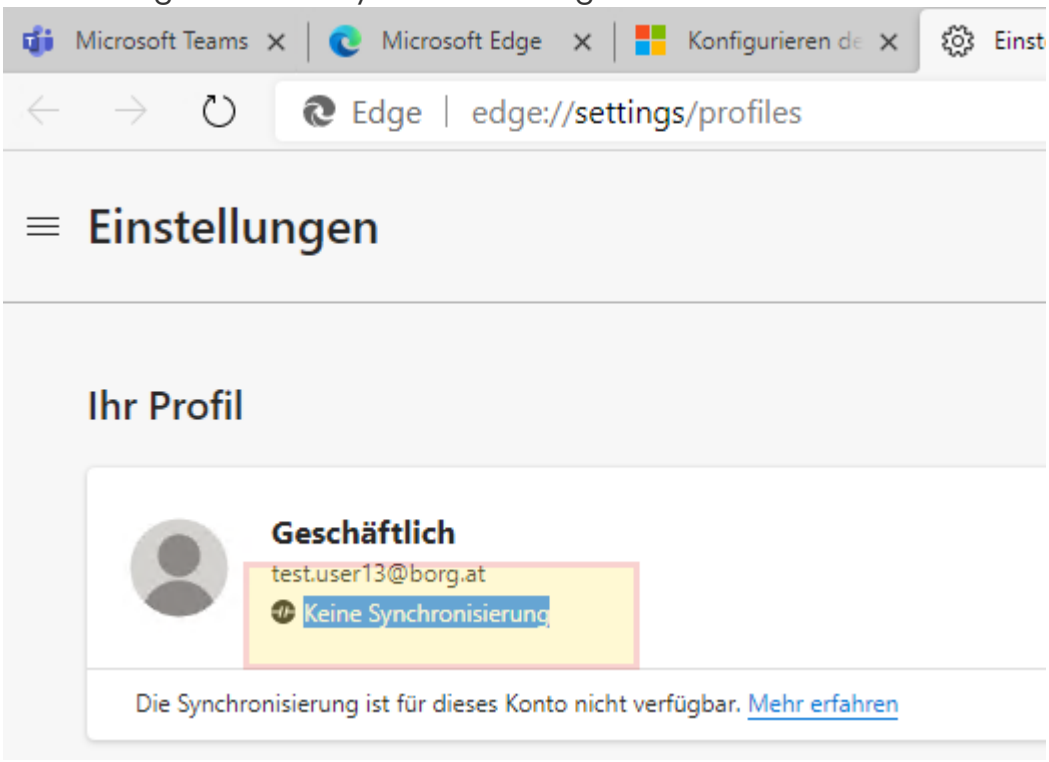


Im Anschluss muss so lange gewartet werden, bis das MSI Paket vollständig hochgeladen ist, davor darf die Seite nicht gewechselt bzw. aktualisiert werden.

8 Unter Umständen auftretende Fehler und deren Lösung

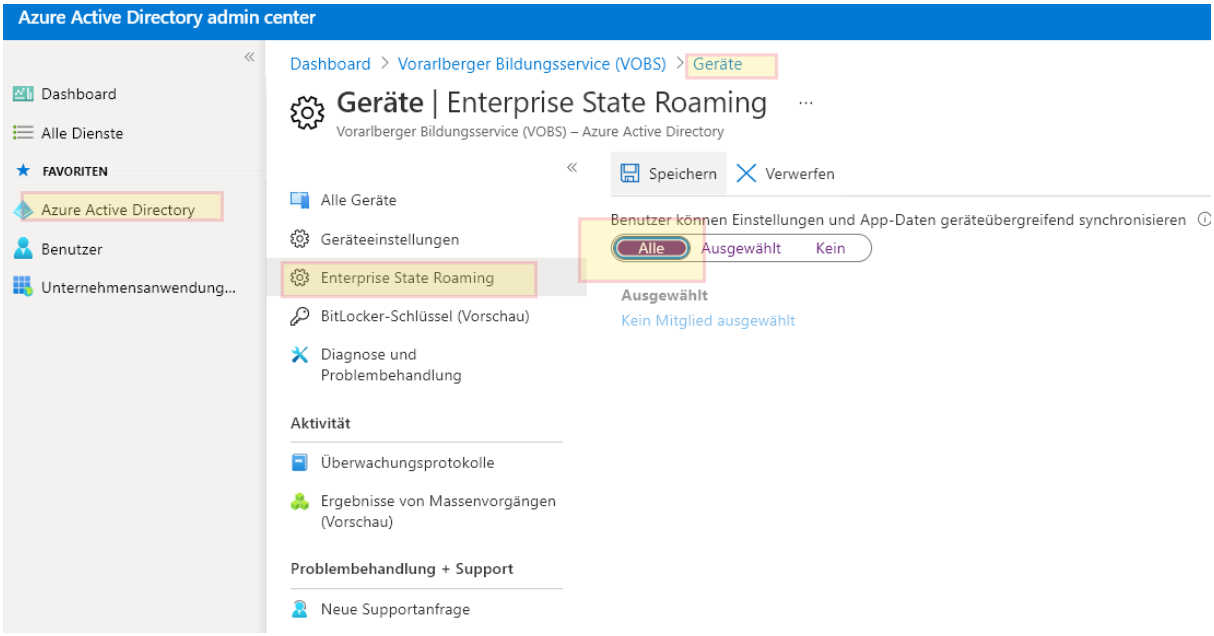
8.1 MS Edge Synchronisierung nicht möglich

Bei MS Edge kann die Synchronisierung vom Benutzer nicht aktiviert werden:



Lösung:
Im Azure Active Directory Admin Portal > Azure Active Directory > Geräte > Enterprise State Roaming

> Alle



Zweite Lösung (globaler Admin-Zugang muss bekannt sein): https://blog.andreas-schreiner.de/2020/03/18/microsoft-edge-account-sync-fehler-sync-isnt-available-for-this-account/

★Erstellt: 2025-11-17 13:15:59 UTC von Lukas Franz
✎Zuletzt aktualisiert: 2025-12-02 08:34:08 UTC von Martin Schnetzer