

WINDOWS DEVICES - 1 - INTUNE ERSTINSTALLATION

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

© 2021 IT-Regionalbetreuer Vorarlberg
6900 Bregenz, Römerstraße 14
Alle Rechte vorbehalten



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

Domäne

schule.at



Testen



CNAME ist für "schule.at" ordnungsgemäß konfiguriert.

- 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

Name ↑	Verfügbare Lizen...	Zugewiesene Lizenzen	Kontotyp
 Microsoft 365 A3 für Lehrpersonal	1	0/1	Organisation
 Microsoft 365 A3 für Schüler und Studenten	1	0/1	Organisation

Admin-Center: Alle Admin Center



Compliance



Endpunkt-Manager



Intune



Intune für Bildungseinrichtungen

Schule



Intune für Bildungseinrichtungen

Schule

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 (Pflicht – bekommen wir vom Lieferanten)
- Windows Product ID (für den Import über eine CSV-Datei nicht erforderlich)
- Hardware Hash (Pflicht – 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 bestimmten 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 Gerätenamen 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 Gerätenamen 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

Vorname

MDM

Nachname

Admin|

Anzeigename *

MDM Admin

Benutzername *

mdmadmin

Domänen

@  ✓

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“.

Alle nach Kategorie anzeigen

Andere

- ☐ Abrechnungsadministrator ⓘ
- ☐ Dienstsupportadministrator ⓘ

Geräte

- ☐ Cloudgeräteadministrator ⓘ
- ☐ Desktop Analytics-Administrator ⓘ
- ☐ Druckeradministrator ⓘ
- ☐ Druckertechniker ⓘ
- ☒ 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

The screenshot displays the Microsoft Admin Center interface. On the left, the 'Aktive Benutzer' (Active Users) section is visible, with a list of users. The user 'MDM...' is selected, and a red box highlights the selection checkbox. The main panel shows the user's profile with various tabs: 'Konto', 'Geräte', 'Lizenzen und Apps', 'E-Mail', and 'OneDrive'. The 'Konto' tab is active, showing details such as the username and email address, the last login, and the user's role (Global Administrator). A red box highlights the 'Multi-Faktor-Authentifizierung' (Multi-Factor Authentication) section, which includes a link to 'Multi-Faktor-Authentifizierung verwalten' (Manage Multi-Factor Authentication).

✓ MFA aktivieren MFA deaktivieren MFA erzwingen MFA-Einstellungen für Benutzer

🔍 × Status : Alle Ansicht : Benutzer

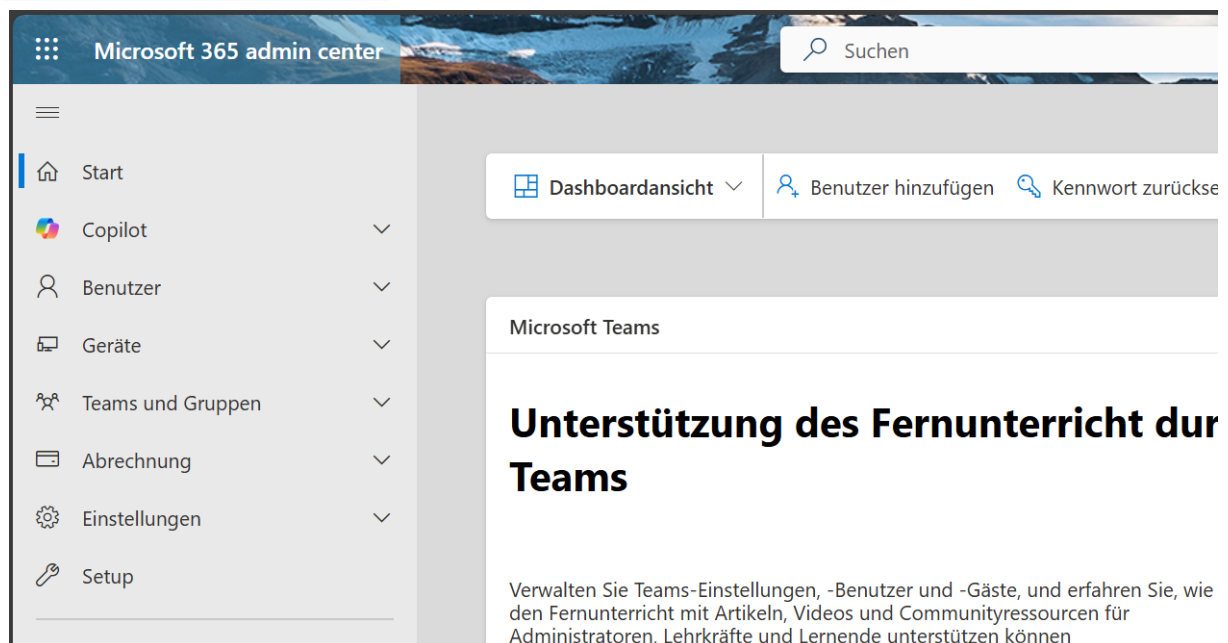
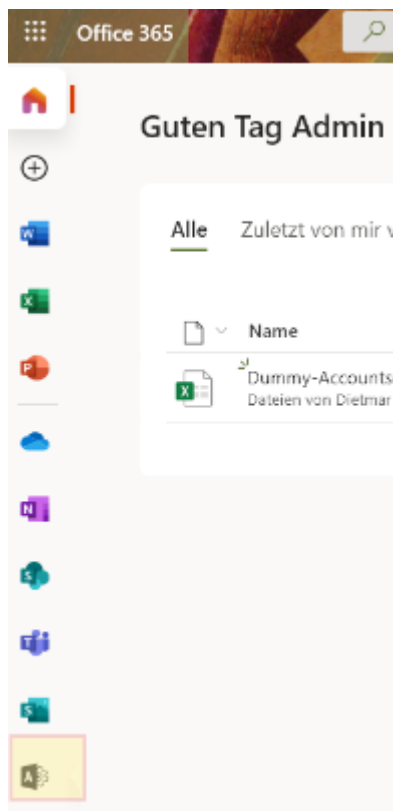
✓	Name ↕	UPN	Status
✓		.at	disabled

2 Die verschiedenen Plattformen

2.1 Die allgemeine MS-365-Verwaltungsoberfläche:

<https://m365.cloud.microsoft>

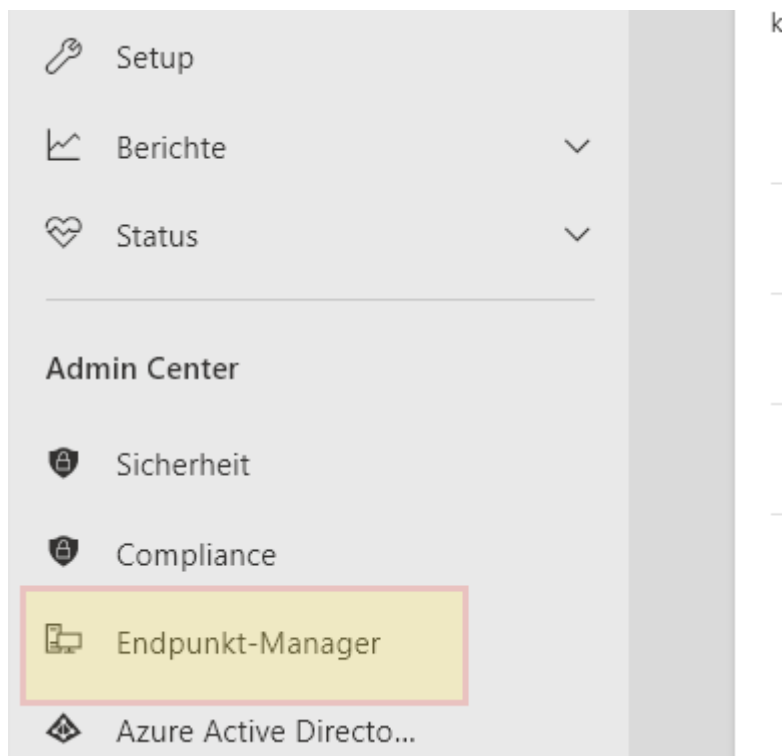
Login als MS365-Administrator:



2.2 Microsoft Intune Admin Center (ehemals Endpoint Manager)

Mit dem neuen Lizenzmodell (ab Juli 2021) auf Basis von „Microsoft 365 A3“ sind nun auch die Lizenzen für das Gerätemanagement enthalten: „Microsoft Endpoint Manager“, 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.

Name	Beschreibung
Azure Active Directory	Intensivieren Sie die bearbeiten Sie das Fi
Compliance	Verwalten Sie Ihre Cc Zugriffssteuerung, el
Endpoint-Manager	Eine einzelne Verwalt Microsoft 365-Geräte
Exchange	Verwalten erweiterte
Power Automatisieren	Verwalten Sie die Au Verbindungen zu We
Office-Konfiguration	Verwalten, konfigurie
Search & intelligence	Microsoft Search-Ein sind. Gestalten Sie di
Stream	Wählen Sie aus, wie I
OneDrive	Kontrollieren von Zu
Power-Apps	Verwenden Sie das P Power Apps, die eine
Intune für Bildungseinrichtungen	Schulgeräte mit dies eingerichtet sind, um
School Data Sync	SDS synchronisiert Si O365-Gruppen, Team Richtlinieneneinstellung

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“).

	Microsoft 365-App	Verwalten, konfigurieren und überwachen Sie die Bereitstellung vor
	Microsoft Entra	Verwenden Sie das Microsoft Entra Admin Center, um Identitäten, E
	Microsoft Purview	Verwenden Sie das Microsoft Purview-Portal, um Datensicherheit, D Daten über mehrere Cloudplattformen und Apps hinweg zu verwal

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 Privatgerätregistrierung 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

The screenshot shows the Microsoft Endpoint Manager Admin Center interface. The left-hand navigation pane has a 'Geräte' (Devices) menu item highlighted with a red box. The main content area shows the breadcrumb path: 'Home > Geräte > Geräte registrieren', with 'Geräte registrieren' also highlighted by a red box. Below this, the 'Registrierungseinschränkungen – Geräteplattform' (Registration restrictions – Device platform) section is active. Under the 'Geräteplattform' (Device platform) tabs, 'Windows-Einschränkungen' (Windows restrictions) is selected and highlighted with a red box. In the 'Einschränkungen zum Gerätetyp' (Restrictions by device type) table, the 'Name' column shows 'Alle Benutzer' (All users), which is also highlighted with a red box.

Priorität	Name	Zugewiesen
Standard	Alle Benutzer	Ja

> Eigenschaften

Microsoft Endpoint Manager Admin Center

Home > Geräte > Geräte registrieren >

Alle Benutzer

Suchen (STRG+ /)

Übersicht

Verwalten

Eigenschaften

Erstellt : A

Letzte Änderung : A

Einschränkung bearbeiten:

Microsoft Endpoint Manager Admin Center

Home > Geräte > Geräte registrieren > Alle Benutzer >

Einschränkung bearbeiten

Gerätetypeneinschränkung

1 Plattformeinstellungen 2 Überprüfen und speichern

Legt die Einschränkungen in Bezug auf Plattformkonfigurationen fest, die für ein Gerät erfüllt werden müssen, damit das Gerät registriert werden kann. Verwenden Sie Konformitätsrichtlinien, um Geräte nach der "Hauptversion.Nebenversion.Build"-Versionseinschränkungen gelten nur für Geräte, die beim Unternehmensportal registriert sind. Intune stuft Geräte standardmäßig als privat ein. Um Geräte als Unternehmens mehr.

Typ	Plattform	Versionen	Persönliches Eigentum
Android Enterprise (Arbeitsprofil)	Erteilen Sie Blockieren	Zulässiger Bereich für Mindestversion/maximale Version: Min. Max.	Erteilen Sie Blockieren
Android-Geräteadministrator	Erteilen Sie Blockieren	Zulässiger Bereich für Mindestversion/maximale Version: Min. Max.	Erteilen Sie Blockieren
iOS/iPadOS	Erteilen Sie Blockieren	Zulässiger Bereich für Mindestversion/maximale Version: Min. Max.	Erteilen Sie Blockieren
macOS	Erteilen Sie Blockieren	Einschränkung nicht unterstützt	Erteilen Sie Blockieren
Windows (MDM)	Erteilen Sie Blockieren	Zulässiger Bereich für Mindestversion/maximale Version: Min. Max.	Erteilen Sie Blockieren

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“:

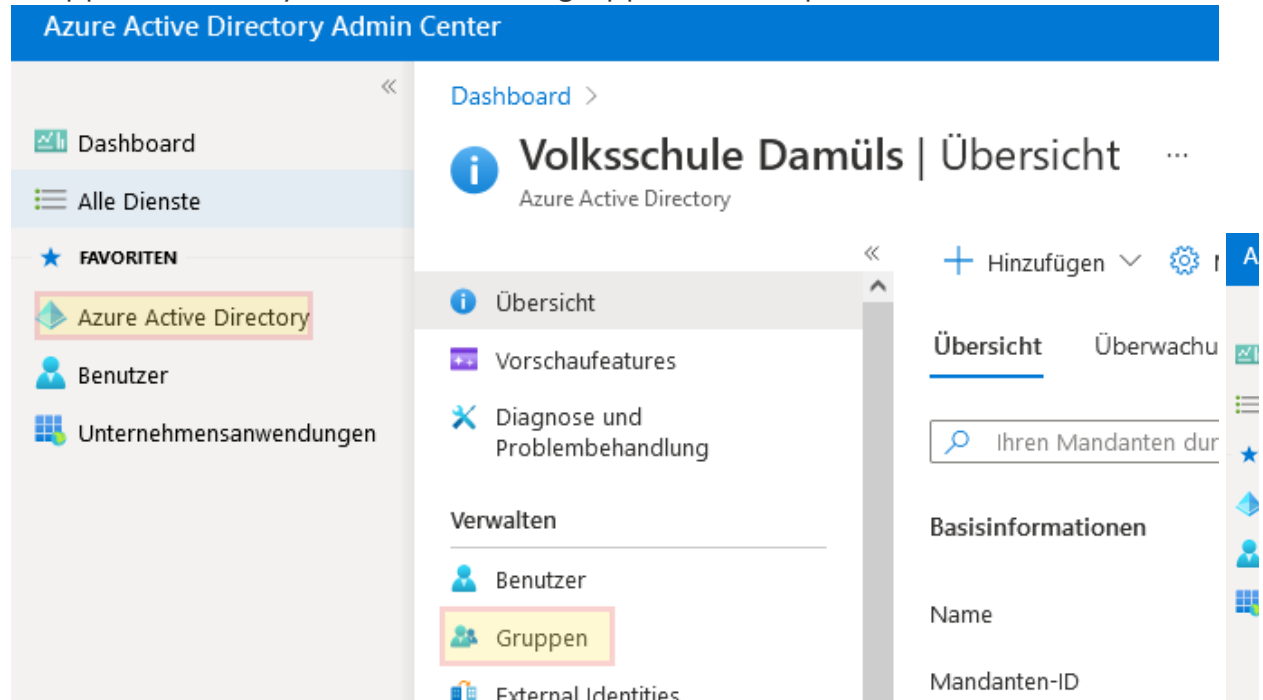


Umso wichtiger ist die Aktivierung der mehrstufigen Authentifizierung für Admin-Konten!

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_“.

Neue Gruppe ...

Gruppentyp * ⓘ

Sicherheit

Gruppenname * ⓘ

C_Autopilot

Gruppenbeschreibung ⓘ

alle per Autopilot registrierten Geräte landen in dieser Gruppe

Azure AD-Rollen können der Gruppe zugewiesen werden (Vorschau) ⓘ

Ja

Nein

Mitgliedschaftstyp * ⓘ

Dynamisches Gerät

Besitzer

Keine Besitzer ausgewählt.

Dynamische Gerätemitglieder * ⓘ

Dynamische Abfrage hinzufügen

Regelsyntax – rechts unten „Bearbeiten“:

Regeln für dynamische Mitgliedschaft ...

Speichern Verwerfen | Haben Sie Feedback für uns?

Regeln konfigurieren

Regeln überprüfen (Vorschau)

Sie können den Regel-Generator oder das Textfeld "Regelsyntax" unten verwenden, um eine Regel für dynamische Mitgliedschaften zu erstellen oder zu bearbeiten. ⓘ [Weitere Informationen](#)

und/Oder	Eigenschaft	Operator	Wert
	<Eigenschaft auswählen>	<Operator auswähl...	Wert hinzufügen

[+ Ausdruck hinzufügen](#)

Regelsyntax

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 "[ZTID]"))
```


Regelsyntax bearbeiten

Sie können Regeln schreiben und/oder direkt bearbeiten, indem Sie die Syntax vorgenommenen Änderungen möglicherweise nicht im Regel-Generator auf d

Regelsyntax ⓘ

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

atio

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:

Gruppen | Alle Gruppen (Vorschau) ...

BORG Egg – Azure Active Directory

« + Neue Gruppe ↓ Gruppen herunterladen 🗑️ Löschen ↻ Aktualisieren ⌵ Spalten 📄 Vorschaufeatures | <

Alle Gruppen (Vorschau)

Gelöschte Gruppen

Diagnose und Problembehandlu...

Einstellungen

Allgemein

Ablaufdatum

...

Diese Seite enthält Vorschauversionen, die Ihnen zum Testen zur Verfügung stehen. Vorschauversionen anzeigen →

Gruppen durchsuchen 🔍 Filter hinzufügen

301 Gruppen gefunden

	Name	↑↓ Objekt-ID	Gruppentyp	Mitgliedschaftstyp
☐	C_Autopilot	b665bffa-c743-4229-9aa2-fea...	Sicherheit	Dynamisch
☐	16 ai Deutsch	0db4075e-27ac-4bf0-a58f-4f4...	Microsoft 365	Zugewiesen

Eigenschaften > Dynamische Mitgliedschaftsregeln

 **C_Autopilot | Dynamische Mitgliedschaftsregeln** ...

Gruppe

«

 Speichern

 Verwerfen

|

 Haben Sie Feedback für uns?

Übersicht

Diagnose und Problembehandlung

Verwalten

Eigenschaften

Mitglieder

Besitzer

Rollen und Administratoren

Verwaltungseinheiten

Gruppenmitgliedschaften

Anwendungen

Lizenzen

Azure-Rollenzuweisungen

Dynamische Mitgliedschaftsregeln

Regeln konfigurieren

Regeln überprüfen (Vorschau)

Sie können den Regel-Generator oder das Textfeld "Regelsyntax" unten verwenden

und/Oder	Eigenschaft
	devicePhysicalIds

+ Ausdruck hinzufügen

Regelsyntax

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

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

Neue Gruppe ...

Gruppentyp * ⓘ

Sicherheit

Gruppenname * ⓘ

C_T21LuL

Gruppenbeschreibung ⓘ

alle Lehrer-Windows Tablets die im Schuljahr 21/22 an die Schule geliefert wurden

Azure AD-Rollen können der Gruppe zugewiesen werden ⓘ

Ja

Nein

Mitgliedschaftstyp * ⓘ

Dynamisches Gerät

Besitzer

Keine Besitzer ausgewählt.

Dynamische Gerätemitglieder * ⓘ

Dynamische Abfrage hinzufügen

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 BILDUNGSSERV...

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_LuL

C_N20SuS
Ausgewählt

C_N21LuL

C_N21SuS
Ausgewählt

C_NaRitlonker

Ausgewählte Elemente

C_N20SuS

Entfernen

C_N21SuS

Entfernen

Auswählen

3.4 Autopilot-Profil 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“

[Home](#) > [Geräte](#) > [Geräte registrieren](#) > [Windows AutoPilot Deployment-Profile](#) >

Profil erstellen

Windows-PC

1 Grundlegende Einstellungen 2 Windows-Willkommenseite 3 Zuweisungen 4 Überprüfen

Name *

T21LuL_Autopilot

Beschreibung

Alle Zielgeräte in Autopilot-Geräte konvertieren ⓘ

Nein

Ja

i Standardmäßig kann dieses Profil nur auf Autopilot-Geräte angewendet werden, die vom Autopilot-Dienstsynchronisiert werden. [Erfahren Sie mehr.](#)

Zurück

Weiter

Beschreibung z. B.: Lehrergeräte Schuljahr 2021/2022

Option 1:

Windows-Willkommensseite – bei LuL: „Benutzergesteuert“

Profil erstellen ...

Windows-PC

✓ Grundlegende Einstellungen

2 Windows-Willkommensseite

3 Zuweisungen

4 Überprüfen + erstellen

Konfigurieren Sie die Willkommensseite für Ihre Autopilot-Geräte.

Bereitstellungsmodus * ⓘ Benutzergesteuert

Azure AD beitreten als * ⓘ In Azure AD eingebunden

Microsoft Software-Lizenzbedingungen ⓘ Anzeigen Ausblenden

ⓘ [Wichtige Informationen zum Ausblenden von Lizenzbedingungen](#)

Datenschutz Einstellungen ⓘ Anzeigen Ausblenden

ⓘ [Der Standardwert für die Sammlung von Diagnosedaten wurde für Geräte geändert, auf denen Windows 10, Version 1903 und höher, oder Windows 11 ausgeführt wird.](#)

Optionen zur Kontoänderung ausblenden ⓘ Anzeigen Ausblenden

Art des Benutzerkontos ⓘ Administrator Standard

Willkommensseite ohne Benutzerauthentifizierung zulassen ⓘ Nein Ja

Sprache (Region) ⓘ Deutsch (Österreich)

Tastatur automatisch konfigurieren ⓘ Nein Ja

Vorlage für Gerätenamen anwenden ⓘ Nein Ja

Erstellen Sie einen eindeutigen Namen für Ihre Geräte. Die Namen dürfen höchstens 15 Zeichen umfassen und nur Buchstaben (a–z, A–Z), Ziffern (0–9) und Bindestriche enthalten. Namen dürfen nicht ausschließlich Ziffern enthalten. Verwenden Sie das Makro "%SERIAL%", um eine hardware-spezifische Seriennummer hinzuzufügen. Alternativ dazu können Sie über das Makro "%RAND:x%" eine zufällige Zeichenfolge von Ziffern hinzuzufügen, wobei x der hinzuzufügenden Anzahl von Ziffern entspricht.

Namen eingeben * 21L-%SERIAL%

Zurück Weiter

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-Willkommen

Eingeschlossene Gruppen

 Gruppen hinzufügen + Alle Geräte hinzufügen

Gruppen

Keine Gruppen ausgewählt

Ausgeschlossene Gruppen

 Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen "Ausschließen" nicht gemischt verwenden. [Klicken Sie hier, um weitere Informationen zu erhalten.](#)

+ Gruppen hinzufügen

Gruppen

Keine Gruppen ausgewählt

Zurück

Weiter

Azure AD-Gruppen

 Suche

 C_Autopilot

 C_T20SuS

 C_T21LuL
Ausgewählt

 C_T21SuS

 grpMS365_D

 grpMS365_L

 grpMS365_S

Ausgewählte Elemente

 C_T21LuL

Auswählen

Profil erstellen ...

Windows-PC

✓ Grundlegende Einstellungen

✓ Windows-Willkommenseite

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“

Profil erstellen ...

Windows-PC

1 Grundlegende Einstellungen

2 Windows-Willkommenseite

3 Zuweisungen

4 Überprüfe

Name *

T20SuS_Autopilot

Beschreibung

Schülergeräte Eintrittsschuljahr 2020 2021

Alle Zielgeräte in Autopilot-Geräte
konvertieren ⓘ

Nein

Ja

i Standardmäßig kann dieses Profil nur auf Autopilot-Geräte angewendet werden, die vom Autopilot-Dienst synchronisiert werden. [Erfahren Sie mehr.](#)

Zurück

Weiter

Name: T20SuS_Autopilot

Beschreibung: Schülergeräte Eintrittsschuljahr 2020 2021

Windows-Willkommensseite – bei SuS „Benutzergesteuert“

Windows-PC

Konfigurieren Sie die Willkommensseite für Ihre Autopilot-Geräte.

Bereitstellungsmodus * ⓘ

Azure AD beitreten als * ⓘ

Microsoft Software-Lizenzbedingungen ⓘ

i Wichtige Informationen zum Ausblenden von Lizenzbedingungen

Datenschutzeinstellungen ⓘ

i Der Standardwert für die Sammlung von Diagnosedaten wurde für Geräte geändert, auf denen Windows 10, Version 1903 und höher, oder Windows 11 ausgeführt wird.

Optionen zur Kontoänderung ausblenden ⓘ

Art des Benutzerkontos ⓘ ☒ Administrator ☐ Standard

Willkommensseite ohne Benutzerauthentifizierung zulassen ⓘ ☒ Nein ☐ Ja

Sprache (Region) ⓘ

Tastatur automatisch konfigurieren ⓘ ☐ Nein ☒ Ja

Vorlage für Gerätenamen anwenden ⓘ ☐ Nein ☒ Ja

Erstellen Sie einen eindeutigen Namen für Ihre Geräte. Die Namen dürfen höchstens 15 Zeichen umfassen und nur Buchstaben (a–Z, A–Z), Ziffern (0–9) und Bindestriche enthalten. Namen dürfen nicht ausschließlich Ziffern enthalten. Verwenden Sie das Makro "%SERIAL%", um eine hardware-spezifische Seriennummer hinzuzufügen. Alternativ dazu können Sie über das Makro "%RAND:x%" eine zufällige Zeichenfolge von Ziffern hinzufügen, wobei x der hinzuzufügenden Anzahl von Ziffern entspricht.

Namen eingeben *

Namen ergeben: 20S-%SERIAL%

Eingeschlossene Gruppen: „C_T20SuS“

Eingeschlossene Gruppen

 Gruppen hinzufügen + Alle Geräte hinzufügen

Gruppen

C_T20SuS

Entfernen

Ausgeschlossene Gruppen

 Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen in den Optionen "Einschließen" und "Ausschließen" nicht gemischt verwendet werden. [Klicken Sie hier, um weitere Informationen zu erhalten.](#)

+ Gruppen hinzufügen

Zurück

Weiter

> 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:

Windows AutoPilot Deployment-Profile ...

Windows-Registrierung

+ Profil erstellen ▾

Mit den Windows AutoPilot Deployment-Profilen können Sie die Willkommensseite für Ihre Geräte anpassen. [Erfahren Sie mehr.](#)

Name	↕	Beschreibung	Jointyp	Zugewiesen
T21LuL_Autopilot		Lehrergeräte SJ 2021 2022	In Azure AD eingebunden	Ja
T20SuS_Autopilot		Schülergeräte Eintrittsschuljahr 2020 2021	In Azure AD eingebunden	Ja
T21SuS_Autopilot		Schülergeräte Eintrittsschuljahr 2021 2022	In Azure AD eingebunden	Ja

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

4 Richtlinien und Konfigurationen:

4.1 Konformitätsrichtlinien

Intune – Geräte - Konformitätsrichtlinien:

Microsoft Endpoint Manager admin center

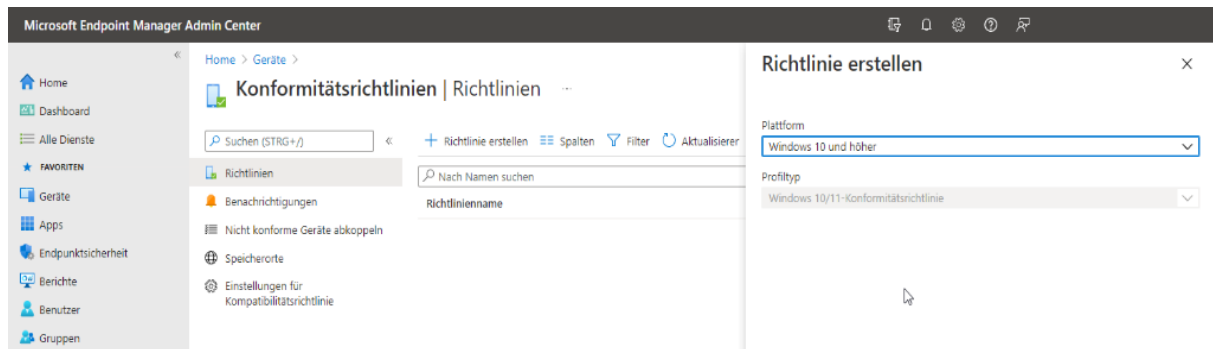
Home > Geräte >

Konformitätsrichtlinien | Richtlinien ...

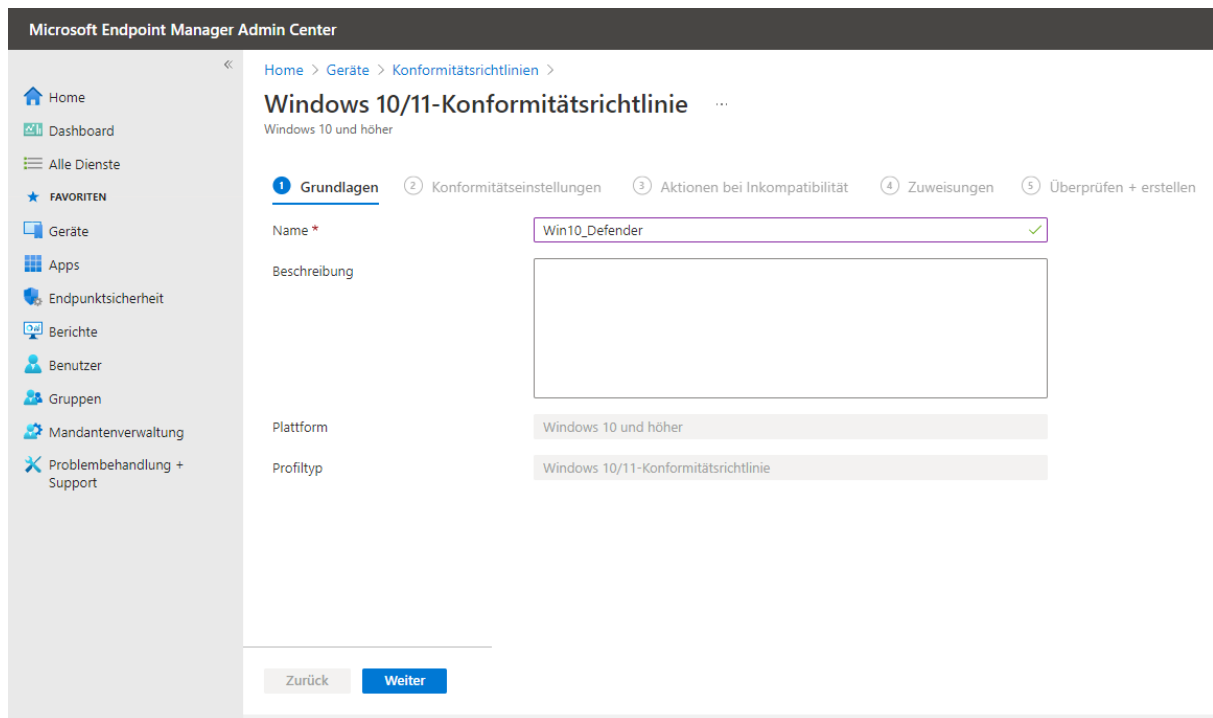
🔍 Suchen (STRG+/) << + Richtlinie erstellen ⌵ Spalten 🔍 Filter

📄 Richtlinien 🔍 Nach Namen suchen

> Erstellen



Plattform: Windows 10 oder höher > Erstellen



Name: Win10_Defender > Weiter

[Home](#) > [Geräte](#) > [Konformitätsrichtlinien](#) >

Windows 10/11-Konformitätsrichtlinie ...

Windows 10 und höher

^ Systemsicherheit

Kennwort

Kennwort zum Entsperren mobiler Geräte erforderlich ⓘ

Anfordern

Nicht konfiguriert

Einfache Kennwörter ⓘ

Blockieren

Nicht konfiguriert

Kennworttyp ⓘ

Gerätestandard

Mindestlänge für Kennwort ⓘ

4

Antispyware ⓘ

Nicht konfiguriert

Defender

Microsoft Defender-Antischadsoftware ⓘ

Anfordern

Nicht konfiguriert

Mindestversion der Microsoft Defender-Antischadsoftware ⓘ

Nicht konfiguriert

Sicherheitsinformationen zu Microsoft Defender-Antischadsoftware auf dem neuesten Stand ⓘ

Anfordern

Nicht konfiguriert

Echtzeitschutz ⓘ

Anfordern

Nicht konfiguriert

✓ Microsoft Defender für Endpunkt

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

Kontrolle: Konformitätsrichtlinie auswählen > Eigenschaften:

[Home](#) > [Geräte](#) > [Konformitätsrichtlinien](#) > [Win10_Defender](#)

Win10_Defender | Eigenschaften

Richtlinie zur Gerätekompatibilität

Übersicht

Verwalten

Eigenschaften

Monitor

Gerätestatus

Benutzerstatus

Status pro Einstellung

Grundlagen [Bearbeiten](#)

Name

Win10_Defender

Beschreibung

--

Plattform

Windows 10 und höher

Profiltyp

Windows 10-Kompatibilitätsrichtlinie

Konformitätseinstellungen [Bearbeiten](#)

Microsoft Defender-Antischadsoftware

Anfordern

Echtzeitschutz

Anfordern

Aktionen bei Inkompatibilität [Bearbeiten](#)

Aktion	Zeitplan
Gerät als nicht konform markieren	Sofort

Bereichstags [Bearbeiten](#)

Standard

Zuweisungen [Bearbeiten](#)

Eingeschlossene Gruppen

C_Autopilot

Ausgeschlossene Gruppen

--

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:

Zuweisungen [Bearbeiten](#)

Eingeschlossene Gruppen	Alle Geräte
Ausgeschlossene Gruppen	--

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 Folgendem verwendet werden können. Verwenden Sie eine Vorlage, wenn Sie Richtlinien nicht manuell 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 Gerät

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 ⓘ

Vertrauenswürdige Zertifikate ⓘ

VPN ⓘ

Windows-Integritätsüberwachung ⓘ

WLAN ⓘ

Erstellen

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

[Home](#) > [Geräte](#) >

×

WLAN ...

Windows 10 und höher

1 Grundlagen

2 Konfigurationseinstellungen

3 Zuweisungen

4 Anwendbarkeitsregeln

5 Überprüfen + erstellen

Name *

EDU-Work ✓

Beschreibung

WLAN für die Geräte aus der Geräteinitiative ✓

Plattform

Windows 10 und höher

Profiltyp

WLAN

Zurück

Weiter

WLAN-Typ: Basis

WLAN

Windows 10 und höher

1 Grundlagen 2 **Konfigurationseinstellungen** 3 Zuweisungen 4 Anwendbarkeitsregeln 5 Überprüfe

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

Zurück

Weiter

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:

✓ Grundlagen ✓ Konfigurationseinstellungen **3 Zuweisungen** ④ Anwe

Eingeschlossene Gruppen

👤 Gruppen hinzufügen 👤 Alle Benutzer hinzufügen + Alle Geräte hinzufügen

Gruppen

C_T20SuS

C_T21SuS

Ausgeschlossene Gruppen

> Weiter > Weiter > Erstellen

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

WLAN ...

Windows 10 und höher

✓ Grundlagen ✓ Konfigurationseinstellungen **3 Zuweisungen** ④ Anwendbarkeitsre

Eingeschlossene Gruppen

👤 Gruppen hinzufügen 👤 Alle Benutzer hinzufügen + Alle Geräte hinzufügen

Gruppen

C_SuS

Ausgeschlossene Gruppen

i Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen in den Optionen "Einschließen" und "Ausschließen" nicht gemischt verwenden. [Klicken Sie hier, um weitere Informationen zum Ausschließen von Gruppen zu erhalten.](#)

Zurück

Weiter

Kontrolle:

Home > Geräte

Geräte | Konfigurationsprofile ...

Suchen (STRG+ /)	«	+ Profil erstellen	≡ Spalten	↻ Aktualisieren	↓ Exportieren	🔍 Filter
Übersicht		Nach Namen suchen				
Alle Geräte		Profilname	↑↓ Plattform	↑↓ Profiltyp	↑↓ Zugewiesen	
Monitor		Freigegebene PC-Richtli...	Windows 10 und höher	Freigegebenes, von mehr...	Ja	
Geräteregistrierung		iOS-Standardgerätrichtl...	iOS/iPadOS	Geräteeinschränkungen	Ja	
Geräte registrieren		Richtlinie für Editionsugp...	Windows 10 und höher	Editionsupgrade und Mod...	Ja	
Wird bereitgestellt		Standardrichtlinien für E...	Windows 10 und höher	Geräteeinschränkungen	Ja	
Windows 365		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
Proxysteinstellungen 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.

The screenshot shows the Azure Active Directory Admin Center interface. On the left is a navigation pane with options like Dashboard, Alle Dienste, and FAVORITEN. The main area displays the 'Übersicht' (Overview) page for the tenant 'Mittelschule Altach'. A yellow box highlights the 'Mandanten-ID' (Tenant ID) field, which contains the value '5160496-...'. A yellow arrow points to this field. To the right of the table, there are links for 'Benutzer', 'Gruppen', 'Anwender', and 'Geräte'.

Basisinformationen	
Name	Mittelschule Altach
Mandanten-ID	5160496-...
Primäre Domäne	ms-altach.at
Lizenz	Azure AD Premium P1

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

Profil erstellen



Plattform

Windows 10 und höher



Profiltyp

Einstellungskatalog (Vorschau)



Starten Sie ganz neu, und wählen Sie die gewünschten Einstellungen aus der Bibliothek der verfügbaren Einstellungen aus.

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

wir nach Einstellungen mit „OneDrive“:

Home > Geräte > Profil erstellen ...
Windows 10 und höher - Einstellungskatalog (Vorschau)

Grundeinstellungen 2 Konfigurationseinstellungen 3 Zuweisungen 4 Bereichstags 5 Überprüfen

Einstellungskatalog
Im Einstellungskatalog können Sie auswählen, welche Einstellungen Sie konfigurieren möchten. Klicken Sie auf "Einstellungen hinzufügen", um den Katalog nach den zu konfigurierenden Einstellungen zu durchsuchen.
[Weitere Informationen](#)

+ Einstellungen hinzufügen

Einstellungsauswahl
Verwenden Sie Kommas (",") in Suchbegriffen, um Einstellungen nach Ihren Schlüsselwörtern zu suchen.
onedrive Suchen

+ Filter hinzufügen

Nach Kategorien durchsuchen
Administrative Vorlagen(Windows-Komponenten)(Microsoft User Experience Virtualization)(Anwendungen)
Microsoft Office 2016(Sonstige)
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:

- ☒ Prevent users from redirecting their Windows known folders to their PC
- ☒ Silently move Windows known folders to OneDrive
- ☒ Silently sign in users to the OneDrive sync app with their Windows credentials

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

Grundeinstellungen 2 Konfigurationseinstellungen 3 Zuweisungen 4 Bereichstags 5 Überprüfen

+ Einstellungen hinzufügen

OneDrive [Kategorie entfernen](#)

37 von 40 Einstellungen in dieser Kategorie sind nicht konfiguriert.

Prevent users from redirecting their Windows known folders to their PC ① ☒ Enabled ⊖

Silently move Windows known folders to OneDrive ① ☒ Enabled ⊖

Show notification to users after folders have been redirected: (Device) * No ✓

Tenant ID: (Device) * ✓

Silently sign in users to the OneDrive sync app with their Windows credentials ① ☒ Enabled ⊖

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 Admin Center

 Home

 Dashboard

 Alle Dienste

 **FAVORITEN**

 Geräte

 Apps

 Endpunktsicherheit

 Berichte

 Benutzer

 Gruppen

 Mandantenverwaltung

 Problembehandlung +
Support

<<

[Home](#) > [Geräte](#)



Geräte | Konfigurati



<<

 Übersicht

 Alle Geräte

 Monitor

Nach Plattform

 Windows

 iOS/iPadOS

 macOS

 Android

Geräteregistrierung



Geräte registrieren

Wird bereitgestellt



Windows 365

Richtlinie



Konformitätsrichtlinien



Bedingter Zugriff



Konfigurationsprofile

„+ Profil erstellen“ mit folgenden Einstellungen:

Profil erstellen



Plattform

Windows 10 und höher



Profiltyp

Einstellungskatalog (Vorschau)



Starten Sie ganz neu, und wählen Sie die gewünschten Einstellungen aus der Bibliothek der verfügbaren Einstellungen aus.

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

[Home](#) > [Geräte](#) >

Profil erstellen

...

Windows 10 und höher - Einstellungskatalog (Vorschau)

1 Grundeinstellungen

2 Konfigurationseinstellungen

3 Zuweisungen

4 Bereichstags

5 Überprüfen + erstellen

Name *

Schuldomäne als Standard für die Anmeldung



Beschreibung

Die Benutzer können sich nur mit dem Benutzernamen und ohne Domäne anmelden.



Plattform

Windows 10 und höher



In den Konfigurationseinstellungen „+ Einstellungen hinzufügen“ auswählen

[Home](#) > [Geräte](#) >

Profil erstellen ...

Windows 10 und höher - Einstellungskatalog (Vorschau)

- ✓ Grundeinstellungen
- 2 Konfigurationseinstellungen**
- ③ Zuweisungen
- ④ Bereichstags
- ⑤ Überprüfen + erstellen



Einstellungskatalog

Im Einstellungskatalog können Sie auswählen, welche Einstellungen Sie konfigurieren möchten. Klicken Sie auf "Einstellungen hinzufügen", um den Katalog nach den zu konfigurierenden Einstellungen zu durchsuchen.

[Weitere Informationen](#)

[+ Einstellungen hinzufügen](#)

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

AAD-Mandantendomäne“ anklicken...

Einstellungsauswahl



Verwenden Sie Kommas (",") in Suchbegriffen, um Einstellungen nach Ihren Schlüsselwörtern zu suchen.

Suchen

+ Filter hinzufügen

Nach Kategorien durchsuchen

> Administrative Vorlagen

Anmeldeinformationsanbieter

Anwendungsstandards

Anwendungssteuerung

Anzeige

Aufgabenplanung

Authentifizierung

Benachrichtigungen

Benutzeroberfläche

Benutzerrechte

Bildung

BitLocker

7 Einstellungen in Kategorie "Authentifizierung"

Alle diese Einstellungen auswählen

Name der Einstellung

☐	AAD-Kennwortzurücksetzung zulassen	ⓘ
☐	EAP-Zertifizierung über SSO zulassen (Benutzer)	ⓘ
☒	Name der bevorzugten AAD-Mandantendomäne	ⓘ
☐	Schnelle erneute Verbindung zulassen	ⓘ
☐	Schnelle erste Anmeldung aktivieren	ⓘ
☐	Sekundäres Authentifizierungsgerät zulassen	ⓘ
☐	Webanmeldung aktivieren	ⓘ

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

[Home](#) > [Geräte](#) >

Profil erstellen



Windows 10 und höher - Einstellungskatalog (Vorschau)

✓ Grundeinstellungen **2 Konfigurationseinstellungen** ③ Zuweisungen ④ Bereichstags ⑤ Überprüfen + erstellen

+ Einstellungen hinzufügen

^ Authentifizierung

Kategorie entfernen

ⓘ 5 von 7 Einstellungen in dieser Kategorie sind nicht konfiguriert.

Name der bevorzugten AAD-Mandantendomäne * ⓘ



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

[Home](#) > [Geräte](#) >

Profil erstellen ...

Windows 10 und höher - Einstellungskatalog (Vorschau)

✓ Grundeinstellungen ✓ Konfigurationseinstellungen **3 Zuweisungen** 4 Bereichstags 5 Überprüfen + erstellen

Eingeschlossene Gruppen

 Gruppen hinzufügen  Alle Benutzer hinzufügen  Alle Geräte hinzufügen

Gruppen

C_Autopilot

[Entfernen](#)

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:

Microsoft Endpoint Manager Admin Center

Home > Endpunktsicherheit

Endpunktsicherheit | Antivirus

Suchen (STRG+ /)

Zusammenfassung Fehlerhafte Endpunkte

Aktualisieren

Letzte Aktualisierung: 4.12.2021, 13:55:56

Fehlerhafte Endpunkte

Update ausstehend	Vollständige Überprüfung...	Nicht...
1	0	0
Offlineüberprüfung ausst...	Kritische Fehler	Inaktiv
0	0	18

AV-Richtlinien

+ Richtlinie erstellen Aktualisieren

Nach Spaltenwert suchen

Richtlinienname	↑↓	Richtlinien
-----------------	----	-------------

Endpunktsicherheit -> Antivirus -> Richtlinie erstellen

Profil erstellen

Endpunktsicherheit | Antivirus

Zusammenfassung

Aktualisieren

Letzte Aktualisierung

Fehlerhafte Endpunkte

Update ausstehend	0
Offlineüberprüfung	0

Aktive Schad...

Keine Gerä...

Plattform

Windows 10, Windows 11 und Windows Server

Profil

Microsoft Defender Antivirus

Microsoft Defender Antivirus

Microsoft Defender Antivirus ist die Schutzkomponente der nächsten Generation von Microsoft Defender für Endpunkt. Sie vereint maschinelles Lernen, Big Data-Analyse, detaillierte Forschung zur Abwehr von Bedrohungen und Cloudinfrastruktur zum Schutz von Geräten in Ihrer Unternehmensorganisation.

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:

^ Defender

Archivüberprüfung zulassen ⓘ	Zugelassen. Überprüft die Archivdateien. ▾
Verhaltensüberwachung zulassen ⓘ	Zugelassen. Aktiviert die Echtzeitverhaltensüberwachung. ▾
Cloudschutz zulassen ⓘ	Zulässig. Aktiviert Cloudschutz. ▾
E-Mail-Überprüfung zulassen ⓘ	Zugelassen. Aktiviert die E-Mail-Überprüfung. ▾
Vollständige Überprüfung auf zugeordneten Netzlaufwerken zulassen ⓘ	Zugelassen. Überprüft zugeordnete Netzwerklaufwerke. ▾
Vollständige Überprüfung von Wechseldatenträgern zulassen ⓘ	Zugelassen. Überprüft Wechseldatenträger. ▾
Eindringenschutzsystem zulassen ⓘ	Zugelassen ▾
Überprüfung aller heruntergeladenen Dateien und Anlagen zulassen ⓘ	Zugelassen ▾
Echtzeitüberwachung zulassen ⓘ	Zugelassen. Aktiviert den Dienst für die Echtzeitüberwachung und fü... ▾
Überprüfung von Netzwerkdateien zulassen ⓘ	Zugelassen. Überprüft Netzwerkdateien. ▾
Skriptüberprüfung zulassen ⓘ	Nicht konfiguriert ▾
Zugriff auf Benutzeroberfläche zulassen ⓘ	Nicht konfiguriert ▾
Faktor für durchschnittliche CPU-Auslastung ⓘ	☒ Nicht konfiguriert
Vor dem Ausführen der Überprüfung auf Signaturen prüfen ⓘ	Nicht konfiguriert ▾
Cloudblockierungsebene ⓘ	Nicht konfiguriert ▾
Erweitertes Cloudtimeout ⓘ	☒ Nicht konfiguriert
Tage zum Beibehalten bereinigter Schadsoftware ⓘ	☒ Nicht konfiguriert

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 ▼

Zugriffsschutz zulassen ⓘ

Wartungsaktion für schwere Bedrohungen

Wartungsaktion für Bedrohungen mit mittlerem Schweregrad

Wartungsaktion für Bedrohungen mit niedrigem Schweregrad

Wartungsaktion für Bedrohungen mit hohem Schweregrad

Zugelassen

Quarantäne: Dateien werden in Quarantäne verschoben

Benutzerdefiniert. Benutzerentscheidung zur auszuführenden Akti...

Benutzerdefiniert. Benutzerentscheidung zur auszuführenden Akti...

Quarantäne: Dateien werden in Quarantäne verschoben

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

⚠ Zu restriktive Einstellungen führen dazu, dass z.B. die Powershell-Skripts, 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 Skripts 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:

Profil erstellen ...

Microsoft Defender Antivirus

✓ Grundlagen ✓ Konfigurationseinstellungen ✓ Bereichstags 4 Zuweisungen 5

Eingeschlossene Gruppen

Gruppen hinzufügen Alle Benutzer hinzufügen + Alle Geräte hinzufügen

Gruppen

Azure AD-Gruppen

Suche

C_ C_Autopilot
C_ C_iPad_alle_ASO

> "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“.

Profil erstellen

×

Plattform

Windows 10 und höher

Profiltyp

Vorlagen

Vorlagen enthalten Gruppen von Einstellungen, die nach Funktionalität angeordnet sind. Verwenden Sie eine Vorlage, wenn Sie Richtlinien nicht manuell erstellen oder Geräte für den Zugriff auf Unternehmensnetzwerke konfigurieren möchten, z. B. durch das Konfigurieren von WLAN oder VPN. [Weitere Informationen](#)

Suchen

Name der Vorlage

Administrative Vorlagen

Benutzerdefiniert

Domänenbeitritt

Mit nachvollziehbarem Namen und entsprechender Beschreibung versehen:

[Home](#) > [Geräte](#) >

Benutzerdefiniert ...

Windows 10 und höher

1 Grundlagen 2 Konfigurationseinstellungen 3 Zuweisungen 4 Anwendbarkeitsregeln 5 Überprüfen + erstellen

Name *	Lokaler Administrator für Lehrergeräte ✓
Beschreibung	Mit diesem Konfigurationsprofil wird ein lokaler Administrator auf den Lehrergeräten eingerichtet. ✓
Plattform	Windows 10 und höher
Profiltyp	Benutzerdefiniert

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>

Zeile hinzufügen



OMA-URI-Einstellungen

Name *	Lokales Administratorkonto ✓
Beschreibung	Nicht konfiguriert
OMA-URI *	./Device/Vendor/MSFT/Accounts/Users/LocalAdmin/Password ✓
Datentyp *	Zeichenfolge ▾
Wert *	P@ssw0rd ✓

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

Zeile hinzufügen



OMA-URI-Einstellungen

Name *

Als Administratorkonto einrichten ✓

Beschreibung

Nicht konfiguriert

OMA-URI *

./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.

Grundlagen ✓ Konfigurationseinstellungen ✓ **3 Zuweisungen** 4 Anwendbarkeitsregeln 5 Überprüfen + erstellen

Eingeschlossene Gruppen

Gruppen hinzufügen Alle Benutzer hinzufügen + Alle Geräte hinzufügen

Gruppen

C_LuL Entfernen

Ausgeschlossene Gruppen

Beim Ausschließen von Gruppen können Benutzer- und Gerätegruppen in den Optionen "Einschließen" und "Ausschließen" nicht gemischt verwenden. [Klicken Sie hier, um weitere Informationen zum Ausschließen von Gruppen zu](#)

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“

[Home](#) > [Geräte](#) >

PowerShell-Skript hinzufügen ...

1 Grundlagen

② Skripteinstellungen

③ Zuweisungen

④ Überprüfen + hinzufügen

Name *

Passwort von LocalAdmin läuft nicht ab



Beschreibung

[Home](#) > [Geräte](#) >

PowerShell-Skript hinzufügen ...

✓ Grundlagen **2 Skripteinstellungen** ③ Zuweisungen ④ Überprüfen + hinzufügen

Skriptspeicherort * ①

AdminPWNotExpiring.ps1



Dieses Skript mit den
Anmeldeinformationen des
angemeldeten Benutzers ausführen ①

Ja

Nein

Skriptsignaturprüfung erzwingen ①

Ja

Nein

Skript in 64-Bit-PowerShell-Host
ausführen ①

Ja

Nein

[Home](#) > [Geräte](#) >

PowerShell-Skript hinzufügen ...

✓ Grundlagen ✓ Skripteinstellungen **3 Zuweisungen** ④ Überprüfen + hinzufügen

Eingeschlossene Gruppen



Gruppen hinzufügen



Alle Benutzer hinzufügen



Alle Geräte hinzufügen

Gruppen

C_N21LuL

Entfernen

Ausgeschlossene Gruppen

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 Gerätenamen 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.

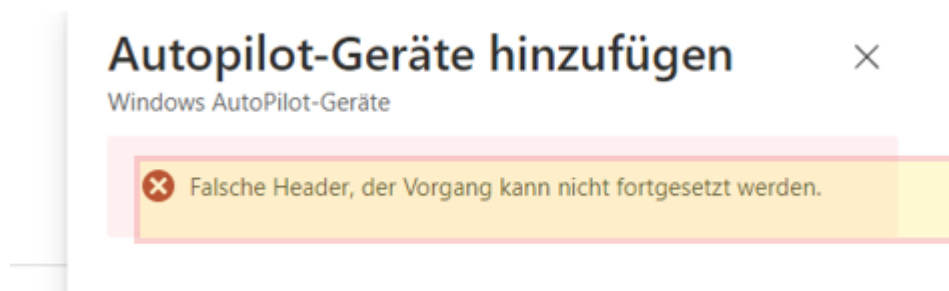
Die Folge ist eine CSV-Datei die zu viele Spalten oder Zeilen enthält. Ersichtlich ist das aber erst, wenn die CSV-Datei mit dem Editor geöffnet wird. Hier sind dann hinten in bei jedem Datensatz zusätzliche Trennzeichen (Strichpunkte bzw.

Beistriche) enthalten – siehe:

ten Ansicht

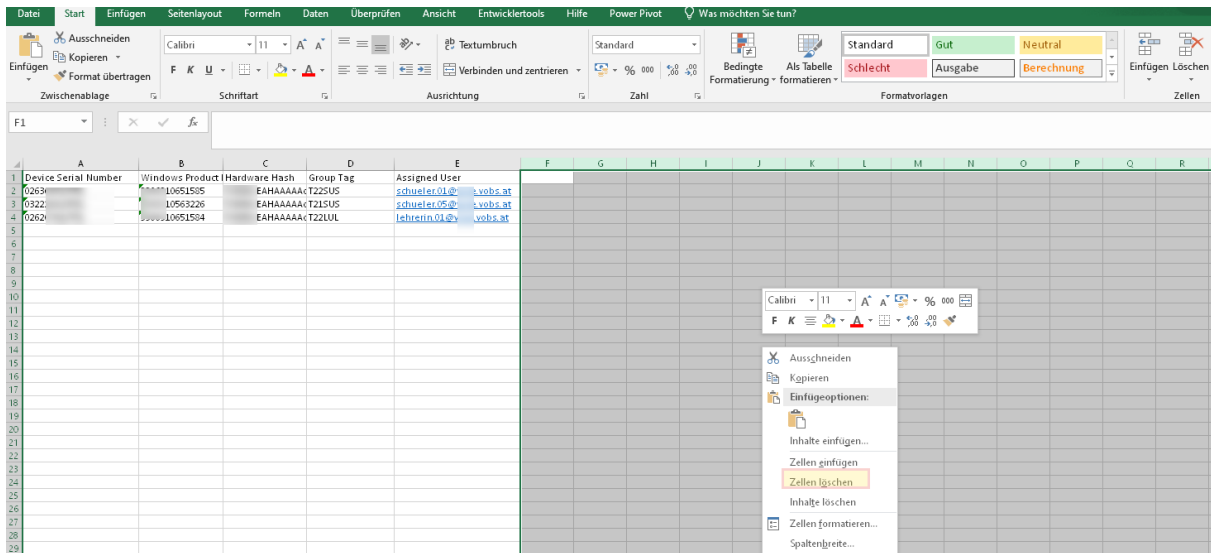
```
ial Number,Windows Product ID,Hardware Hash,Group Tag,Assigned User,
51,,AvA7pHSIu1J3gCCQMCABAACQABAAIABAABAAAABQAZAAgAAAAAA/
cm9zb2Z0IENvcnBvcmlFOaW9uABAAGgBNaWNYb3NvZnQgQ29ycG9yYXRpb24AEQARAFN1cmZhY2UgR28gMg/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAA,T21LuL,u.at,
51,,AvA7pH5/y5J3gCCQMCABAACQABAAIABAABAAAABQAZAAgAAAAAA/
cm9zb2Z0IENvcnBvcmlFOaW9uABAAGgBNaWNYb3NvZnQgQ29ycG9yYXRpb24AEQARAFN1cmZhY2UgR28gMg/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAA,T21LuL,u.at,
51,,AvA7pH5/y5J3gCCQMCABAACQABAAIABAABAAAABQAZAAgAAAAAA/
cm9zb2Z0IENvcnBvcmlFOaW9uABAAGgBNaWNYb3NvZnQgQ29ycG9yYXRpb24AEQARAFN1cmZhY2UgR28gMg/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAA,T21LuL,u.at,
51,,uCGAvA7pH5/y5J3gCCQMCABAACQABAAIABAABAAAABQAZAAgAAAAAA/
cm9zb2Z0IENvcnBvcmlFOaW9uABAAGgBNaWNYb3NvZnQgQ29ycG9yYXRpb24AEQARAFN1cmZhY2UgR28gMg/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/
AAAA,T21LuL,u.at,
```

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



Abhilfe:

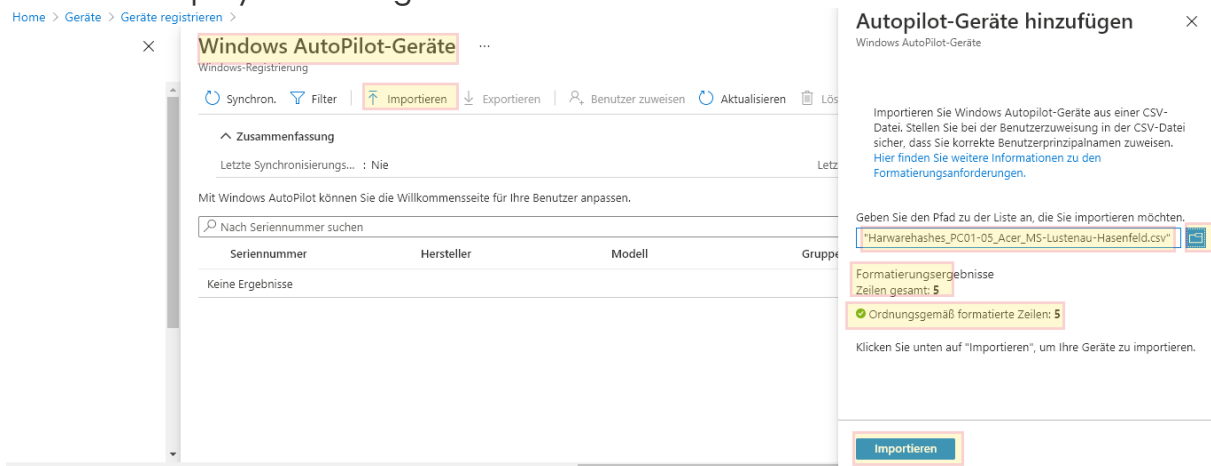
In Excel zusätzlich befüllte Zellen (Spalten und/oder Zeilen) nicht nur „inhaltlich“ löschen, sondern die ganzen Spalten/Zeilen markieren und diese dann löschen. Am besten zur Sicherheit vor dem csv-Export einige der leeren Spalten rechts markieren und mit RK „Zellen löschen“ komplett löschen (dasselbe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



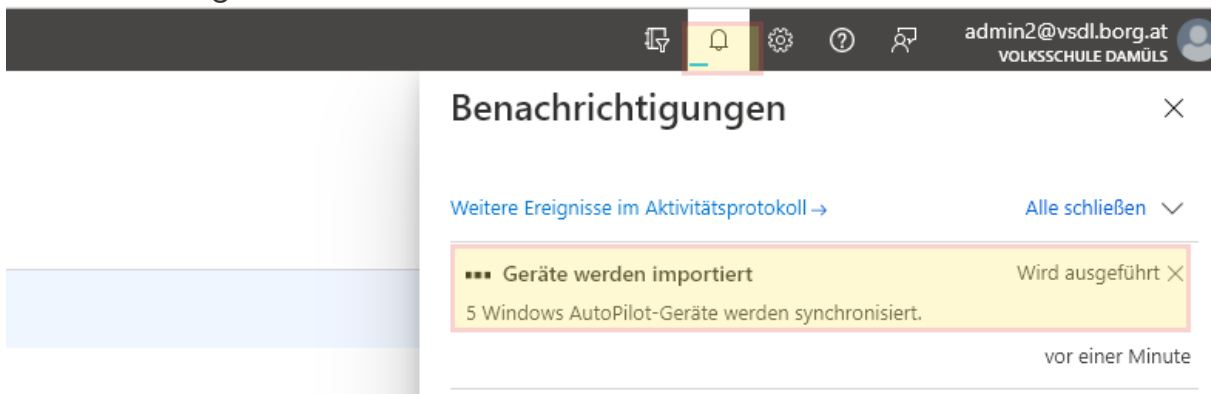
Excelmappe speichern und erst dann den Export machen.

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:

Benachrichtigungen



Weitere Ereignisse im Aktivitätsprotokoll →

Alle schließen ▾



Geräte importiert



5 Windows AutoPilot-Geräte wurden erfolgreich hochgeladen.

Vorerst lautet der Profilstatus „Nicht zugewiesen“:

Windows AutoPilot-Geräte

Windows-Registrierung

Synchron.

Filter

Importieren

Exportieren

Benutzer zuweisen

Aktualisieren

Löschen

^ Zusammenfassung

Letzte Synchronisierungs... : 09.12.21, 22:51

Letzte erfolgreiche Synch... : 09.12.21, 22:51

Mit Windows AutoPilot können Sie die Willkommenseite für Ihre Benutzer anpassen.

Nach Seriennummer suchen

Seriennummer	Hersteller	Modell	Gruppentag	Profilstatus	Bestellung
☐ NXVPNEV002138220177600	Acer	TravelMate P214-53	T21LUL	Nicht zugewiesen.	N/V
☐ NXVPNEV002138222A77600	Acer	TravelMate P214-53	T20SUS	Nicht zugewiesen.	N/V
☐ NXVPNEV002138223287600	Acer	TravelMate P214-53	T21SUS	Nicht zugewiesen.	N/V
☐ NXVPNEV0021382252E7600	Acer	TravelMate P214-53	T21LUL	Nicht zugewiesen.	N/V
☐ NXVPNEV002138225E07600	Acer	TravelMate P214-53	T21LUL	Nicht zugewiesen.	N/V

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

☐ NXVPNEV002138220177600	Acer	TravelMate P214-53	T21LUL	Wird aktualisiert
☐ NXVPNEV002138222A77600	Acer	TravelMate P214-53	T20SUS	Wird aktualisiert
☐ NXVPNEV002138223287600	Acer	TravelMate P214-53	T21SUS	Wird aktualisiert
☐ NXVPNEV0021382252E7600	Acer	TravelMate P214-53	T21LUL	Wird aktualisiert
☐ NXVPNEV002138225E07600	Acer	TravelMate P214-53	T21LUL	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:

Seriennummer	Hersteller	Modell	Gruppentag	Profilstatus
☐ NXVPNEV002138220...	Acer	TravelMate P214-53	T21LUL	Zugewiesen
☐ NXVPNEV002138222...	Acer	TravelMate P214-53	T20SUS	Zugewiesen
☐ NXVPNEV002138223...	Acer	TravelMate P214-53	T21SUS	Zugewiesen
☐ NXVPNEV002138225...	Acer	TravelMate P214-53	T21LUL	Zugewiesen
☐ NXVPNEV002138225...	Acer	TravelMate P214-53	T21LUL	Zugewiesen

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

NXVPNEV0021382...
Windows AutoPilot-Geräte

Benutzer ⓘ

lehrerin.01@vsdl.borg.at

Seriennummer ⓘ

NXVPNEV002138220177600

Hersteller ⓘ

Acer

Modell ⓘ

TravelMate P214-53

Gerätename ⓘ

Gruppentag ⓘ

T21LUL

Profilstatus ⓘ

Zugewiesen

Zugewiesenes Profil ⓘ

T21LuL_Autopilot

Zuweisungsdatum ⓘ

09.12.21, 22:54

Registrierungsstatus ⓘ

Nicht angemeldet

Zugeordnetes Intune-Gerät ⓘ

N/V

Zugeordnetes Azure AD-Gerät ⓘ

[NXVPNEV002138220177600](#)

Zuletzt kontaktiert ⓘ

Nie

- 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 Gerätenamen kommt dann erst mit der tatsächlichen Verbindung des Gerätes mit dem Internet und der 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

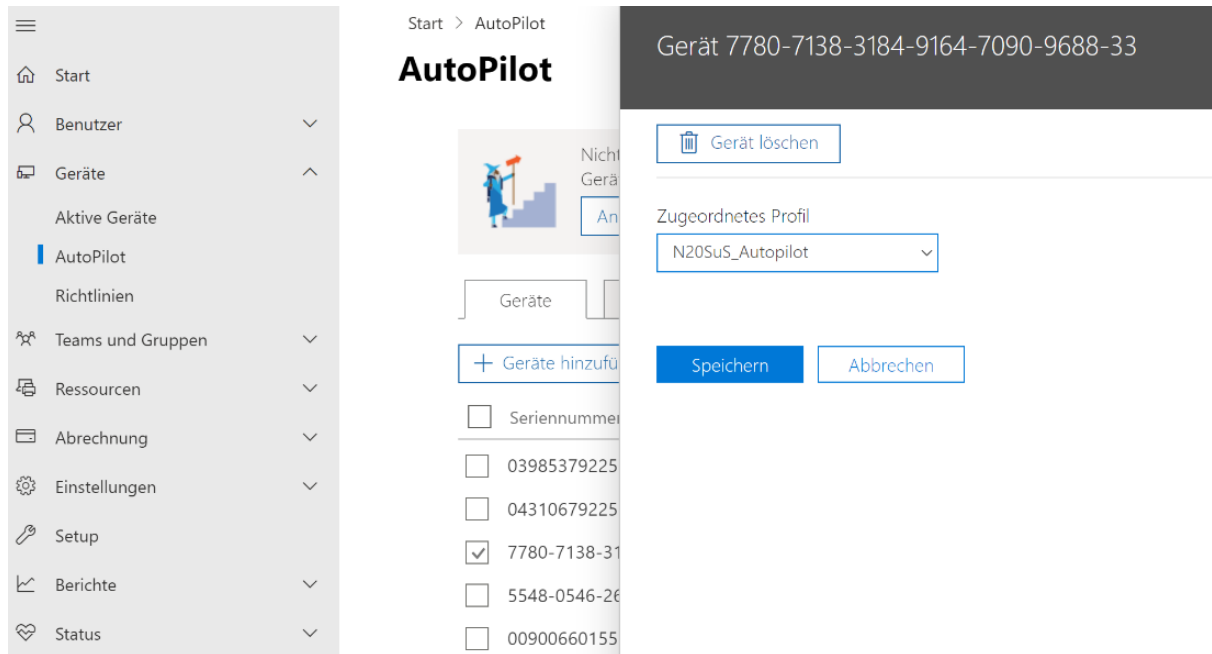
Name	L1-P201THUE
Geräte-ID	10894171-d126-4197-9cd2-6d5850075e23 
Objekt-ID	05438059-13c7-4258-a4e7-1706adbbe77d 
Aktiviert	Ja
Betriebssystem	Windows
Version	10.0.19043.1348
Jointyp	Azure AD joined
Besitzer	test lehrer
Benutzername	testlehrer@ms-altach.at
MDM	Microsoft Intune
Konform	Ja
Registriert	7.1.2021, 09:10:40
Aktivität	19.12.2021, 09:59:19
Gruppen	C_Autopilot , C_N21LuL , C_Bitlocker
Erweiterungsattribute	Keine Erweiterungsattribute

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:

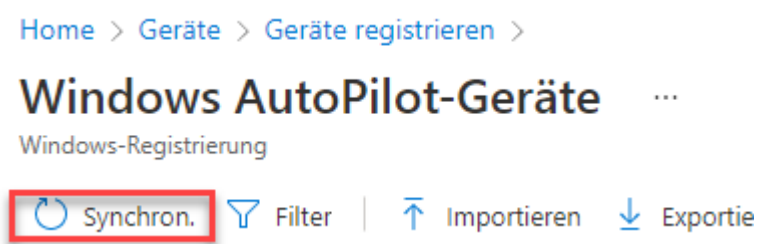
Microsoft 365 admin center > Geräte > Autopilot > Gerät auswählen und Profil zuordnen



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“:

Microsoft Endpoint Manager Admin Center

Home > Geräte > Geräte registrieren >

Seite "Registrierungsstatus" ...

Windows-Registrierung

[+ Erstellen](#)

Die Seite zum Registrierungsstatus wird bei der anfänglichen Geräteeinrichtung und der ersten Benutzeranmeldung aktiviert, wenn diese Option aktiviert ist, können Benutzer den Konfigurationsfortschritt der zugewiesenen Apps und Profile anzeigen. [Erfahren Sie mehr.](#)

Priorität	Name	Zugewiesen
Standard	Alle Benutzer und alle Geräte	Ja

Eigenschaften – Einstellungen bearbeiten:

Verwalten

[Eigenschaften](#)

Name: Alle Benutzer und alle Geräte

Beschreibung: Dies ist die Konfiguration des unabhängigen von der Gruppe aller Benutzer und alle Geräte

Einstellungen [Bearbeiten](#)

Konfigurationsfortschritt für Apps und Profile anzeigen: Nein

Einstellungen:

1 Einstellungen 2 Überprüfen und speichern

Die Seite zum Registrierungsstatus wird bei der anfänglichen Geräteeinrichtung und der ersten Benutzungsanfrage angezeigt. Wenn diese Option aktiviert ist, können Benutzer den Konfigurationsfortschritt der zugewiesenen App anzeigen. [Erfahren Sie mehr.](#)

Konfigurationsfortschritt für Apps und Profile anzeigen

☐ Nein ☒ Ja

Fehler anzeigen, wenn die Installation länger als die angegebene Anzahl von Minuten dauert

Bei einem Zeitlimit oder Fehler benutzerdefinierte Meldung anzeigen

☐ Nein ☒ Ja

Setup konnte nicht abgeschlossen werden. Versuchen Sie es noch mal, oder wenden Sie sich an Ihre IT-Abteilung.

Protokollsammlung und Diagnosesite für Endbenutzer aktivieren

☐ Nein ☒ Ja

Seite nur für Geräte anzeigen, die über die Willkommenseite bereitgestellt wurden

☐ Nein ☒ Ja

Geräteverwendung blockieren, bis alle Apps und Profile installiert sind ⓘ

☒ Nein ☐ Ja

Überprüfen und speichern

Abbrechen

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:

Microsoft Endpoint Manager admin center

Dashboard > Apps > Windows | Windows Apps

+ Hinzufügen Aktualisieren Filter Exportieren Spalten

Angewendete Filter: Plattform, App-Typ

Nach Name oder Herausgeber suchen

Name	↑↓	Typ	Status
Adobe Reader Touch (Online)		Microsoft Store für Unternehmen...	
Excel		Weblink	
Excel Mobile (Online)		Microsoft Store für Unternehmen...	
Fresh Paint (Online)		Microsoft Store für Unternehmen...	

App-Typ auswählen

App erstellen

App-Typ

Windows 10

Store-App

Microsoft Store-App

Microsoft 365-Apps

Windows 10

Microsoft Edge, Version 77 und höher

Windows 10

Sonstige

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

Microsoft 365-Apps hinzufügen

Microsoft 365-Apps (Windows 10)

1 Informationen zur App-Suite 2 App-Suite konfigurieren 3 Zuweisungen 4 Überprüfen + erstellen

Format der Konfigurationseinstellungen

*

Konfigurations-Designer

App-Suite konfigurieren

Office-Apps auswählen ⓘ

8 ausgewählt

Andere Office-Apps auswählen (Lizenz erforderlich) ⓘ

0 ausgewählt

Informationen zur App-Suite

Diese Einstellungen gelten für alle Apps, die Sie in der Suite ausgewählt haben. [Weitere Informationen](#)

Architektur ⓘ

32 Bit

64 Bit

Updatekanal * ⓘ

Halbjährlicher Enterprise-Kanal

Andere Versionen entfernen ⓘ

Ja

Nein

Zu installierende Version ⓘ

Neueste

Spezifisch

Spezifische Version

Aktuelle Version

Eigenschaften

Aktivierung gemeinsam genutzter Computer verwenden ⓘ

Ja

Nein

Microsoft-Softwarelizenzbedingungen im Auftrag von Benutzern akzeptieren

Ja

Nein

Hintergrunddienst für Microsoft Search in Bing installieren ⓘ

Ja

Nein

Sprachen ⓘ

1 Sprache(n) ausgewählt

Zurück

Weiter

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)

[Apps](#) > [Windows](#) >

Microsoft 365-Apps hinzufügen

Microsoft 365-Apps (Windows 10)

✓ Informationen zur App-Suite

✓ App-Suite konfigurieren

3 Zuweisungen

4

Required ⓘ

Gruppenmodus	Gruppe	Filtermodus
+ Enthalten	C_Autopilot	Keine

[+ Gruppe hinzufügen](#) ⓘ [+ Alle Benutzer hinzufügen](#) ⓘ [+ Alle Geräte hinzufügen](#) ⓘ

> 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

[Home](#)
[Dashboard](#)
[Alle Dienste](#)
FAVORITEN
[Geräte](#)
[Apps](#)

Home > Apps >

Windows | Windows Apps

Suchen (BEFEHL+ /)

[+ Hinzufügen](#) [Aktualisieren](#) [Filter](#) [Exportieren](#) [Spalten](#)

Windows Apps

Angewendete Filter: Plattform, App-Typ

Nach Name oder Herausgeber suchen

Name ↑ ↓ Typ

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 App

1 App-Informationen 2 Zuweisungen 3 Überprüfen und erstellen

Datei auswählen *

App-Paketdatei auswählen

App-Paketdatei



App-Paketdatei *

"GeoGebra-Windows-Installer-6-0-672-0.msi"



Name: GeoGebra Classic

Plattform: Windows

Größe: 78,27 MiB

MAM aktiviert: Nein

Ausführungskontext: Pro Benutzer

OK

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.

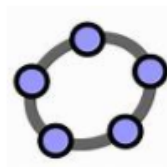
Entwickler ⓘ

Besitzer ⓘ

Hinweise ⓘ

Logo ⓘ

[Bild ändern](#)



Zurück

Weiter

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

> Apps >

App hinzufügen

Branchenspezifische Windows MSI-App

✓ App-Informationen

2 Zuweisungen

3 Überprüfen und erstellen

Erforderlich

Gruppenmodus	Gruppe	Filtermodus
Keine Zuweisungen		
+ Gruppe hinzufügen + Alle Benutzer hinzufügen + Alle Geräte hinzufügen		

Für registrierte Geräte verfügbar

Gruppenmodus	Gruppe	Filtermodus
Keine Zuweisungen		
+ Gruppe hinzufügen + Alle Benutzer hinzufügen		

Deinstallieren

Gruppenmodus	Gruppe	Filtermodus
Keine Zuweisungen		
+ Gruppe hinzufügen + Alle Benutzer hinzufügen + Alle Geräte hinzufügen		

Zurück

Weiter

Gruppen auswählen

Azure AD-Gruppen

C_Autopilot

C_iPad_alle_ASO

C_iPad2020SUS

C_iPad2021LUL

C_iPad2021SUS

C_iPads_801013_StadtschulzentrumBludenz

C_iPads_801023_LUL

Ausgewählte Elemente

Keine Elemente ausgewählt.

Auswählen

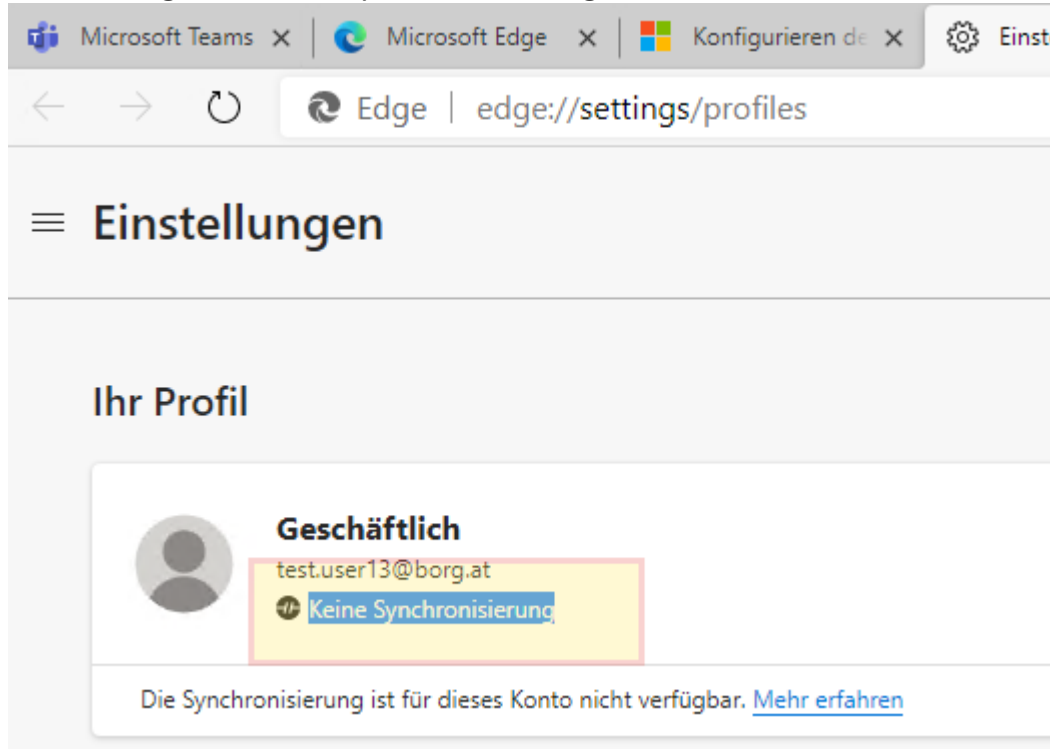
Es muss mindestens 1 Element ausgewählt werden.

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

Azure Active Directory admin center

Dashboard > Vorarlberger Bildungsservice (VOBS) > Geräte

Geräte | Enterprise State Roaming

Vorarlberger Bildungsservice (VOBS) – Azure Active Directory

Speichern Verwerfen

Benutzer können Einstellungen und App-Daten geräteübergreifend synchronisieren ⓘ

Alle Ausgewählt Kein

Ausgewählt
Kein Mitglied ausgewählt

FAVORITEN

- Azure Active Directory
- Benutzer
- Unternehmensanwendung...

Aktivität

- Überwachungsprotokolle
- Ergebnisse von Massenvorgängen (Vorschau)

Problembehandlung + Support

- Neue Supportanfrage

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