AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

Qualifizierung von Systembetreuerinnen
und Systembetreuern

Imaging und
MDM mit Microsoft Endpoint Manager

INHALT

IMPRESSUM

Herausgeber: Akademie für Lehrerfortbildung und Personalführung
Kardinal-von-Waldburg-Str. 6 - 7
89407 Dillingen

Autoren: Thomas Pickel, Maximilian-Kolbe-Schule Neumarkt
Stefan Langer, Reischlesche Wirtschaftsschule Augsburg
Kurt Windberger, ALP

URL: https://alp.dillingen.de/schulnetz
Mail: thomas.pickel@fosbos-neumarkt.de
Stand: Mai 2022

ÜBERSICHT

Für die Installation und Verwaltung von Rechnern mit Windows-Betriebssystem stehen derzeit mehrere Verfahren zur Verfügung, die sich in der Bedienung und dem technischen Aufwand stark voneinander unterscheiden. In diesem Lehrgang sollen drei Möglichkeiten vorgestellt und erprobt werden. Die Wahl des eingesetzten Verfahrens ist abhängig von der Qualifikation des Systembetreuers und den Bedürfnissen der Schule.

Verfahren		Komplexität	Arbeitsaufwand	Einsatzzweck	Kosten
imagebasiertes Klonen	USB-Sticks	niedrig	hoch	kleine selbstverwaltete Netzwerke	kostenlos
	FOG-Server	hoch	mittel	größere selbstverwaltete Netzwerke mit häufigem Imaging	kostenlos
MDM	Microsoft Endpoint Manager	hoch	niedrig	alle Netzwerkgrößen, externe Unterstützung durch Dienstleister möglich	monatliche Gebühren

Die Verfahren mit USB-Sticks oder FOG-Server setzen auf ein „klassisches“ Schulnetzkonzept, bei dem die Daten lokal auf einem Server in der Schule (z. B. einer NAS / Network Attached Storage) gespeichert werden. Größere Schulnetzwerke setzten in der Vergangenheit auch lokale Domänen zur Benutzerverwaltung ein.
Der aktuelle Stand der Technik ist ein Übergang auf Cloudlösungen: Daten werden nicht mehr lokal, sondern z. B. in OneDrive gespeichert. Dadurch entfallen beim Einsatz von Microsoft 365 viele Komponenten klassischer Netzwerke, wie beispielsweise die Konfiguration von Netzlaufwerken.
Ein hybrider Übergang von klassischen Netzwerken zu cloudbasierten Lösungen ist auch schrittweise möglich, z. B. durch den Ersatz von Netzlaufwerken durch Cloudspeicher. Im Rahmen der schulinternen Lehrerfortbildung erscheint es sinnvoll, das Kollegium und die Schüler/innen etappenweise an cloudgestützte Netzwerke heranzuführen.
Die nahezu flächendeckende Einführung von MS Teams hat für viele Schulen bereits den Weg in das Cloud Computing eingeläutet; die Geräteverwaltung kann darauf aufbauen.

ORGANISATORISCHER HINWEIS

In diesem Laborbuch werden alle drei Techniken erläutert. In Präsenzveranstaltungen würden praktische Laborübungen zu allen Bereichen aber den zeitlichen Rahmen sprengen. Deshalb müssen für Kurse inhaltliche Schwerpunkte gesetzt und einige Inhalte nur theoretisch behandelt werden.
Zu diesem Kurs finden Sie auf der Schulnetz-Materialien-Webseite eine ZIP-Datei mit Beispiel-Skripten zum Download.

BEGRIFFSKLÄRUNG

- Unter einem Mobile Device Management (MDM) versteht man ein System zur zentralisierten Verwaltung von mobilen und stationären Endgeräten sowie Apps. Die Verwaltung umfasst dabei die Inventarisierung von Geräten und die Software-, Daten- und Richtlinienverteilung.
- Der Microsoft Endpoint Manager (Intune) ist Microsofts MDM. Es eignet sich besonders zur Verwaltung von Windows-Geräten, kann aber zunehmend besser auch mit Android- und Apple-Geräten umgehen.

WINDOWS-LIZENZIERUNG

Zu den verschiedenen Lizenzmodellen von Microsoft gibt es eine Übersicht auf der Schulnetz-Webseite: https://schulnetz.alp.dillingen.de/materialien/Microsoft_Lizenzmodelle.pdf

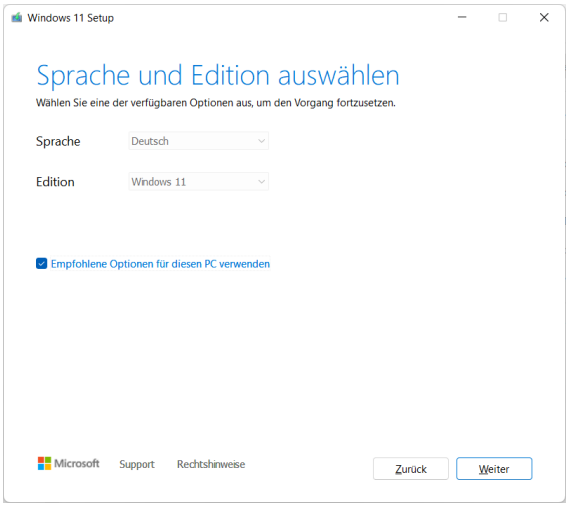
Die überwiegende Zahl der Rechner, die in Schulen eingesetzt werden, verfügen schon ab Werk über eine im BIOS bzw. der UEFI-Firmware vorinstallierte digitale Windows-Lizenz. Bei der Anschaffung ist darauf zu achten, dass eine „Professional“ (Pro)- oder „Education“ (Edu)-Lizenz beschafft wird; Home-Lizenzen (oft auch nur als „Windows 10/11“ ohne Zusatz bezeichnet) können weder mit Microsofts MDM verwaltet noch in lokale Domänen eingebunden werden. Auf Geräten mit digitalen Home -Lizenz können nachträglich Lizenzschlüssel zum Upgrade auf Pro oder Edu eingetragen werden.

EINZELPLATZINSTALLATION VON WINDOWS

ERSTELLEN EINES BOOTMEDIUMS

Das Windows-Betriebssystem wird unter Verwendung des aktuellen „Media Creation Tool“ (MCT), welches bootfähige USB-Sticks erzeugt, selbst erstellt. Benötigt wird ein leerer USB-Stick mit mindestens 8 GB Speicherplatz.

Das MCT kann von der Microsoft-Website heruntergeladen werden (Stichwort: „Erstellen von Installationsmedien für Windows“). Nach Auswahl einiger Optionen arbeitet das Tool selbständig und erstellt den Boot-Stick.



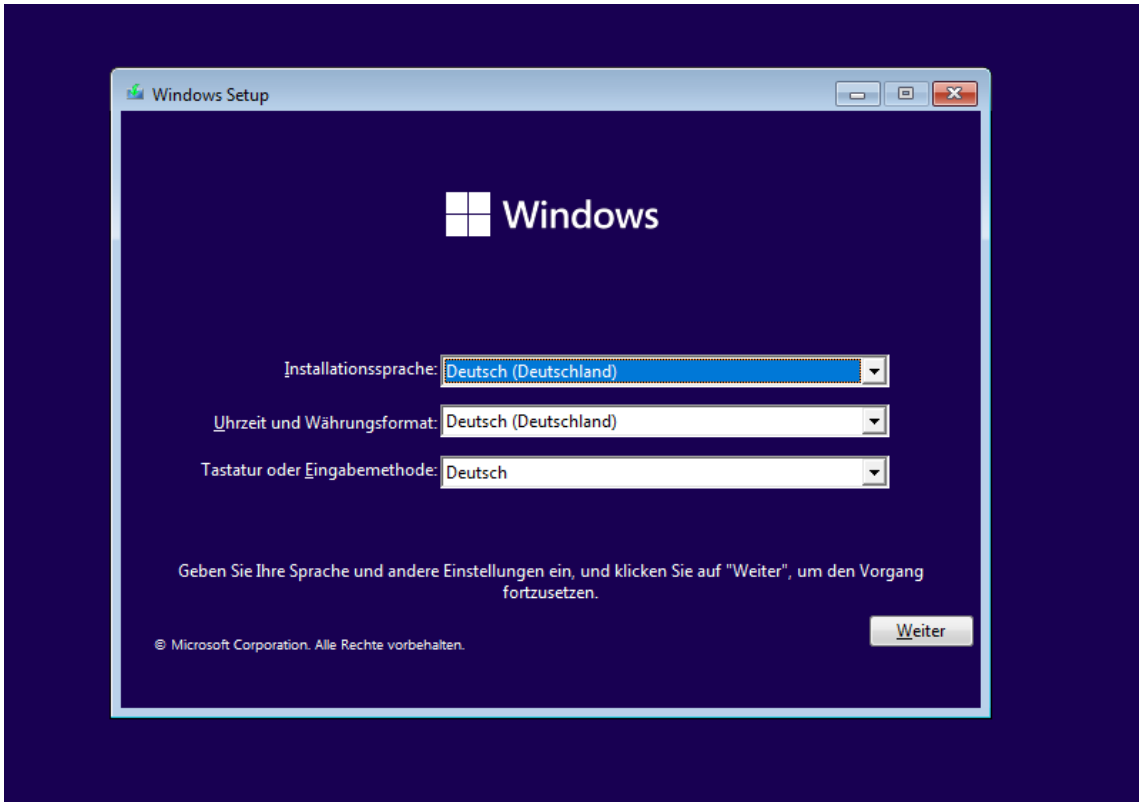
USB-BOOT

Der zu installierende Rechner soll nicht von der eingebauten Festplatte, sondern vom USB-Stick booten. Dafür sind manchmal Eingriffe im BIOS bzw. UEFI notwendig. Sobald der Computer eingeschaltet wird, gelangt man durch wiederholtes Drücken einer bestimmten Taste in das Konfigurationsmenü. Diese Taste ist oft eine der folgenden: ESC, DEL, F1, F2, F8 oder F10.

Der PC soll von USB-Sticks gebootet werden dürfen. Zudem sollte das Bootmenü beim Start aufrufbar sein (oftmals die Taste F12).

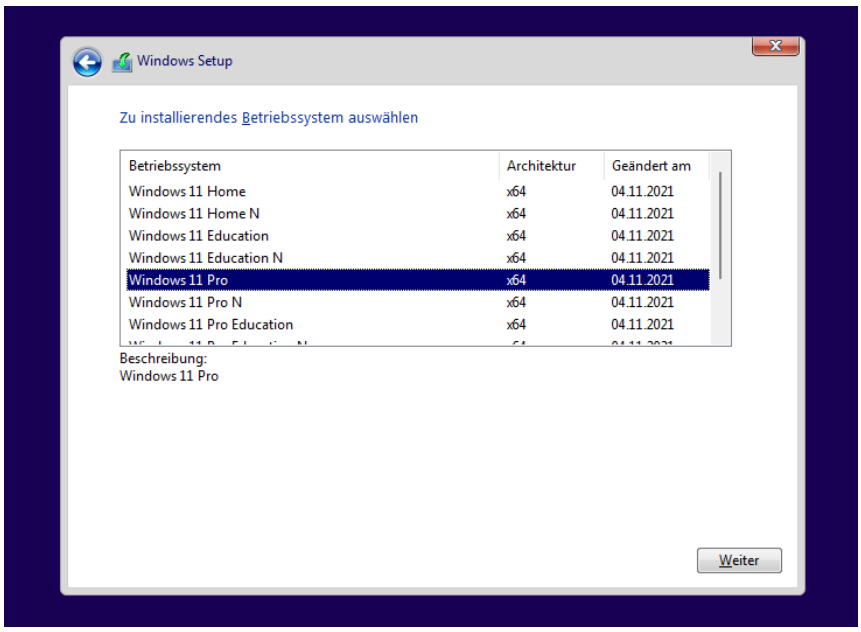
Quelle: https://www.alteeve.com/w/images/thumb/1/18/Fujitsu_BIOS_Main-page.png/665px-Fujitsu_BIOS_Main-page.png

Sobald der PC vom USB-Stick gebootet werden kann, läuft das Windows-Setup an.



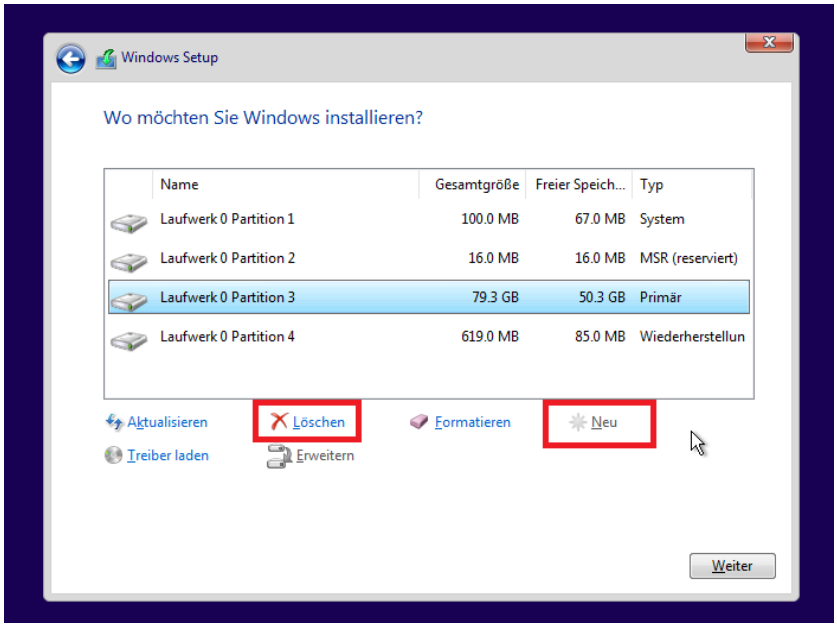
Zunächst wird – falls im BIOS bzw. der UEFI-Firmware des Rechners kein digitaler Lizenzschlüssel hinterlegt ist – ein Product Key abgefragt; hier klickt man in Test- und Schulungssituationen auf „Ich habe keinen Product Key“. Windows läuft für einen Zeitraum von (mindestens) 30 Tagen auch ohne Aktivierung. Digitale Lizenzen werden vom Setup automatisch erkannt, in diesem Fall wird kein Menü zur Auswahl der Windows-Variante eingeblendet.

Bei der Auswahl des Betriebssystems sollte man zu Testzwecken immer die Pro- oder Edu-Version von Windows installieren:



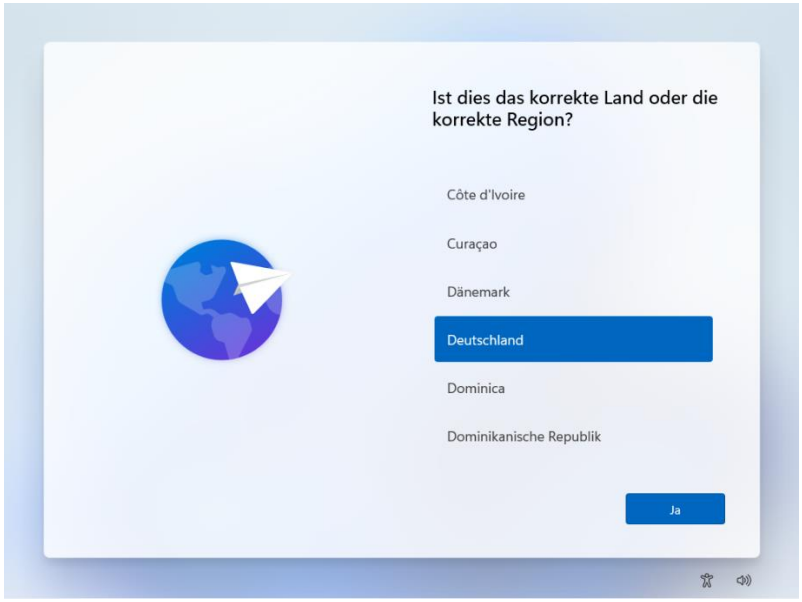
PARTITIONIERUNG DER FESTPLATTE

Die im Gerät verbaute Festplatte wird bei der Betriebssysteminstallation in mehrere Bereiche unterteilt. Windows 11 erstellt standardmäßig vier Partitionen, von denen im Normalbetrieb nur eine sichtbar ist (Laufwerk C:\). Für eine saubere Neuinstallation werden alle Partitionen gelöscht und Windows neu im „unpartitionierten Bereich“ installiert.

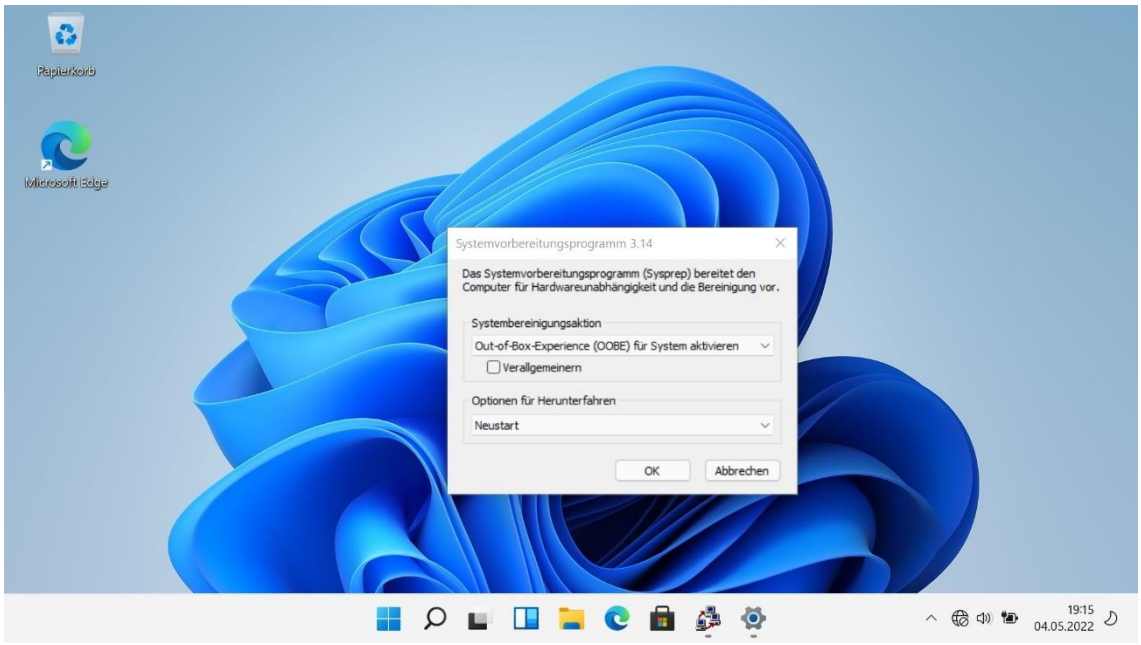


OOBE UND AUDIT-MODE

Der Rest der Installation verläuft seit Windows 10 vollautomatisch und führt direkt zur „Out-of-the-box-experience (OOBE), in der Region, Tastaturlayout, ggf. WLAN-Verbindung, Benutzerkonto etc. abgefragt werden.



Soll eine Musterinstallation zum Klonen von Rechnern installiert werden, muss der Vorgang an dieser Stelle mit der Tastenkombination STRG + Shift + F3 unterbrochen werden; Windows startet sofort im Audit-Modus neu.



In diesem Modus können Programme installiert und Einstellungen vorgenommen werden, wie zum Beispiel:

- Installation von Treibern (geschieht aber i. d. R. automatisch über Windows Update)
- Einpflegen von Windows-Updates
- Entfernen nicht erwünschter Standard-Apps
- Installation von Druckern
- Verbinden von Netzlaufwerken, ggf. über Batchskripte im Autostart-Menü über ein Anmeldeskript
- Installation eines Office-Programms
- Installation weiterer benötigter Programme

Im Audit-Modus dürfen keine Benutzerkonten angelegt werden – das geschieht später beim Versiegeln!

Der Systembetreuer sollte die einzelnen Arbeitsschritte sorgfältig dokumentieren, da Windows-Images in regelmäßigen Abständen (z.B. nach Windows-Upgrades) neu angelegt werden müssen.

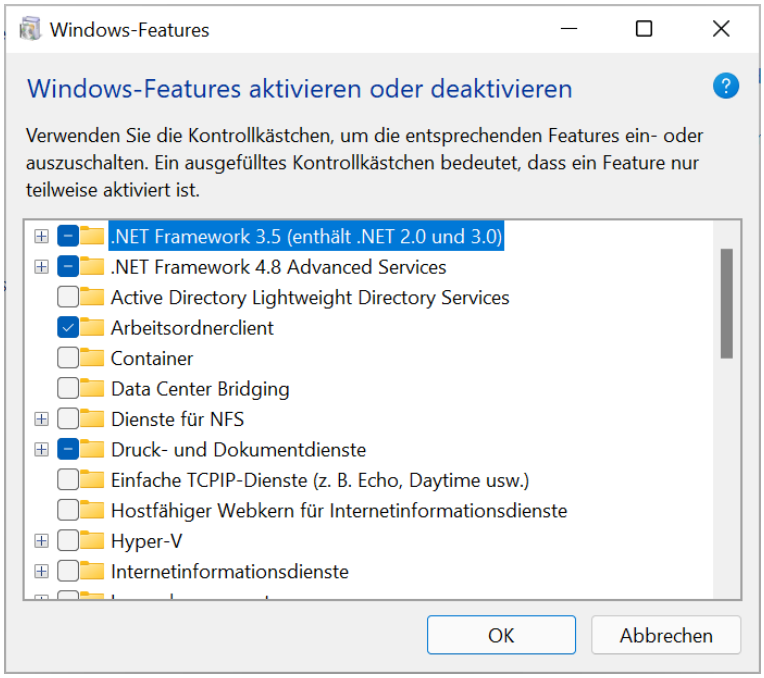
VERSIEGELN DER MUSTERINSTALLATION

Nach Abschluss der Musterinstallation sollte zunächst ein Backup des Systems mit einem Tool wie Drive Snapshot angelegt werden, falls bei den folgenden Schritten ein Fehler passiert.

Wer sich mit Virtualisierungssoftware wie VirtualBox auskennt, sollte statt dessen die gesamte Musterinstallation in einer virtuellen Maschine durchführen und zum Sichern die Snapshot-Funktion der Virtualisierungssoftware verwenden (vgl. https://schulnetz.alp.dillingen.de/materialien/Virtualbox.pdf).

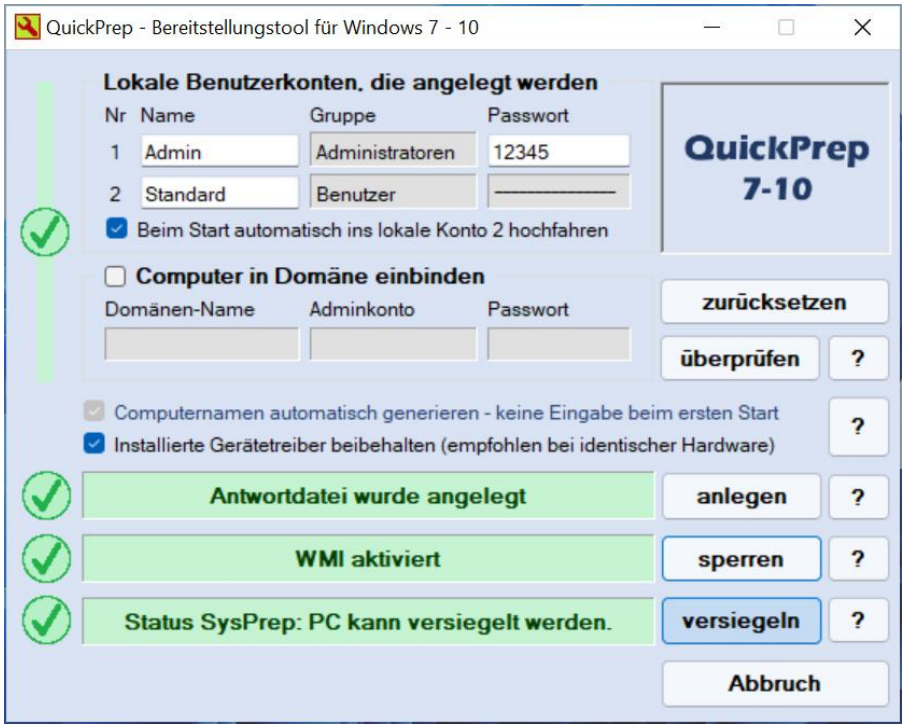
Die Musterinstallation wird nun versiegelt. Da die dafür zuständige Software Sysprep nicht einfach zu konfigurieren ist, ist es ratsam, das Tool „Quickprep“ zu verwenden.
(-> https://schulnetz.alp.dillingen.de/materialien.html)

Quickprep benötigt .Net 3.5, das über Startmenü – Systemsteuerung – Programme – "Windows-Features aktivieren oder deaktivieren" installiert werden kann.



Quickprep wird installiert und gestartet. Zu beachten ist:

- Quickprep funktioniert auch unter Windows 11.
- Es werden zwei Benutzer angelegt, von denen nur der Admin ein Passwort besitzt. Der zweite Benutzer kann sich ohne Passwort einloggen, hat aber keine administrativen Rechte.
- Der Computer kann in eine ggf. vorhandene Domäne aufgenommen werden.



Die Buttons „überprüfen“, „anlegen“, ggf. „sperren“ müssen angeklickt werden. Mit einem Klick auf „versiegeln“ startet der Sysprep-Prozess, der nicht rückgängig gemacht werden kann. Der Rechner wird versiegelt und fährt herunter.

Beim nächsten Start von der Festplatte wird das Betriebssystem „entsiegelt“ und ist nicht mehr als Musterinstallation zu gebrauchen, daher muss unbedingt von einem USB-Stick (bzw. Netzwerk) gebootet werden!

IMAGE-BASIERTE VERFAHREN (KLONEN)

IMAGING MIT MICROSOFT-TOOLS (DISM/IMAGEX)

Das Klonen von Rechnern geschieht in diesem Verfahren mit USB-Bootsticks, mit denen die Images aufgezeichnet und ausgerollt werden. Dies ist für kleine Umgebungen ratsam.

Aufgrund der Häufigkeit von Windows-Updates sollten die Images mindestens einmal im Halbjahr aktualisiert werden. Da Windows-Versionsupdates im Auditmodus nicht installiert werden können, ist üblicherweise eine vollständig neue Musterinstallation notwendig; der Arbeitsaufwand beträgt für einen erfahrenen Systembetreuer und bei guter Dokumentation etwa einen halben Arbeitstag.

NUTZUNG DES WINDOWS-INSTALLATIONSSTICKS

Zum Aufzeichnen der Images kann der im vorangehenden Kapitel erstellte Windows-Installationsstick verwendet werden. Die zusätzlich benötigte Software (z. B. GImageX, Drive Snapshot, Batch-Skripte; siehe unten) wird zusätzlich auf den Stick kopiert. Sobald das System geladen ist, können mit der Tastenkombination „Shift + F10“ eine Eingabeaufforderung geöffnet und die gewünschten Programme gestartet werden.

ERSTELLUNG EINES WINDOWS PE-STICKS

Ein Windows Preinstallation Environment (PE) Boot-Stick kann selbst erstellt werden, siehe die Handreichung https://schulnetz.alp.dillingen.de/materialien/WinPE10.pdf. Zu Schulungszwecken können die Referenten den Teilnehmern einen WinPE-Stick zur Verfügung stellen.

Zu beachten ist, dass der Stick zum Start von UEFI-PCs im FAT32-Format (nicht NTFS) formatiert sein muss; FAT32 erlaubt nur Partitionen bis 32 GB und nur Dateigrößen bis 4GB.

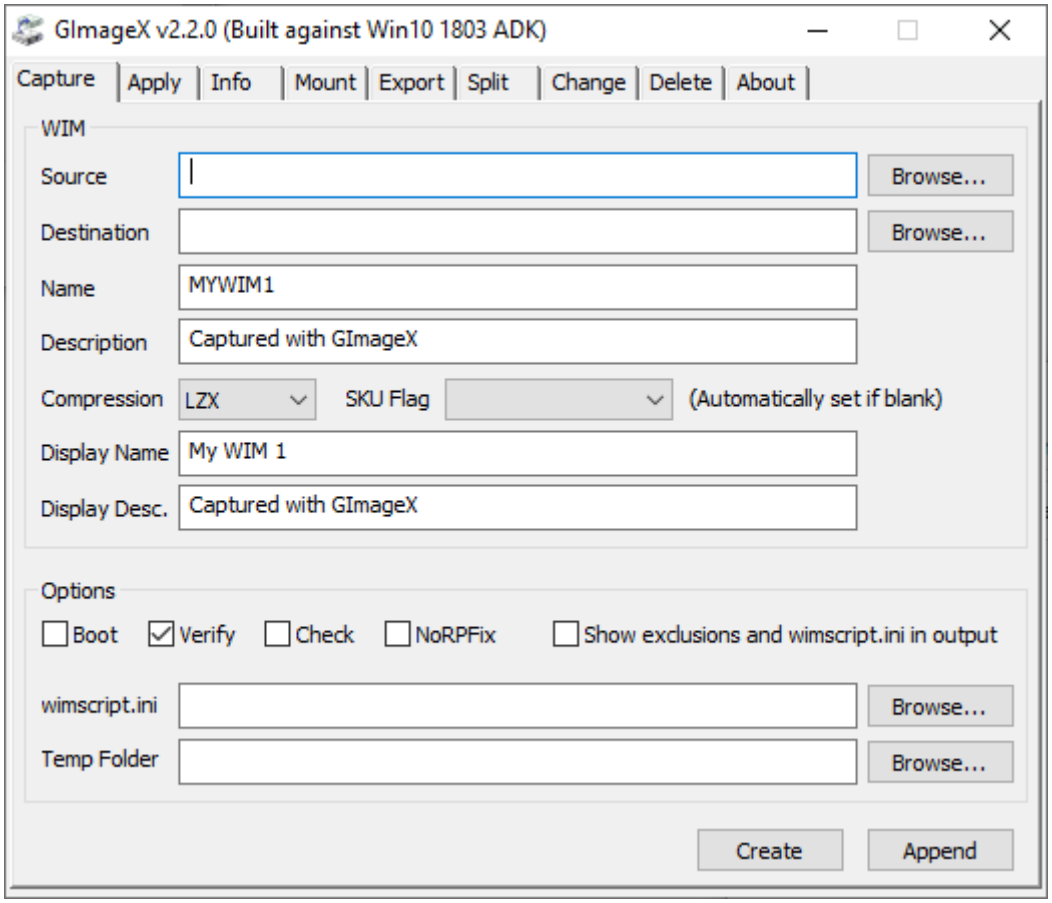
Ein Windows PE-Stick bietet zusätzliche Konfigurationsmöglichkeiten über Batch-Skripte bis hin zum vollautomatisierten Klonen eines Computers.

AUFZEICHNEN EINES IMAGES

Zu diesem Thema liegt eine ausführliche Dokumentation auf der Schulnetz-Seite vor: https://schulnetz.alp.dillingen.de/materialien/DISM.pdf

Für Einsteiger ist es ratsam, das Programm GImageX in der richtigen Version (meist x64) auf den Boot-Stick zu kopieren: https://www.autoitconsulting.com/site/software/gimagex/

Die Software zeichnet im Reiter „Capture“ den Inhalt einer Partition in einer WIM-Datei auf.



AUSROLLEN DES IMAGES

Auch hier wird der zu installierende PC von einem Boot-Stick gestartet. Um eine saubere Installation zu gewährleisten, muss die Festplatte zuerst komplett gelöscht und korrekt partitioniert werden. Hierfür wird das Kommandozeilenprogramm `diskpart` gestartet.

Mit den folgenden Befehlen wird eine GPT-Festplatte vorbereitet:

```
diskpart
DISKPART> list disk
DISKPART> select disk 0
DISKPART> clean
DISKPART> convert gpt
DISKPART> create partition efi size=100
DISKPART> format fs=fat32 quick label="System"
DISKPART> assign letter=s
DISKPART> create partition msr size=16
DISKPART> create partition primary
DISKPART> format fs=ntfs quick label="Windows"
DISKPART> assign letter=w
DISKPART> exit
```

Anschließend wird die aufgezeichnete WIM-Datei mit dem Befehl `dism` auf die korrekte Partition übertragen:

```
dism /apply-image /imagefile:<Quelle> /applydir:<Ziel> /Index:1
```

Beispiel:

```
dism /apply-image /imagefile:z:\win11.wim /applydir:w:\ /Index:1
```

Alternativ könnte an dieser Stelle wieder GImageX eingesetzt werden.

Abschließend muss noch der Bootmanager angelegt werden; dies geschieht mit dem Befehl

```
bcdboot w:\windows /s s:
```

Der geklonte Rechner wird nun durch das Schließen der Eingabeaufforderung oder den Befehl

```
shutdown -r -t 0
```

neu gestartet und durchläuft das in der Musterinstallation eingestellte automatische Setup.

Für das Klonen einer Vielzahl von Rechnern bietet es sich an, den gesamten Vorgang mittels einer Batch-Datei zu automatisieren. Praxisbeispiele entnehmen Sie bitte dem Schulnetz-Skript https://schulnetz.alp.dillingen.de/materialien/DISM.pdf

IMAGING ÜBER SERVER (FOG)

Die Installation und der Betrieb von Free Opensource Ghost (FOG) erfordert vertiefte Netzwerk- und Linux-Kenntnisse. Der erhöhte Aufwand rentiert sich bei größeren Netzwerken und in Situationen, in denen häufig geklont werden muss.

Zunächst wird der FOG-Server auf einer physischen oder virtuellen Maschine installiert, und die entsprechenden Einstellungen für PXE-Boot in den DHCP-Server eingetragen.

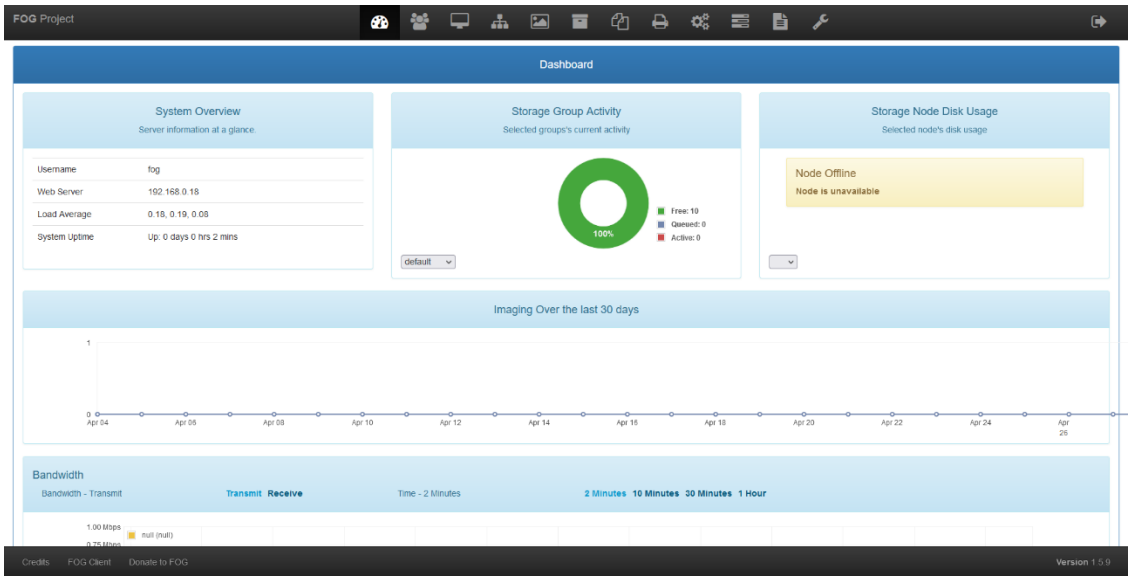
Anschließend wird auf einem PC eine Musterinstallation angelegt. Dieser Rechner wird dann über das Netzwerk gebootet, in FOG registriert und das Image aufgezeichnet.

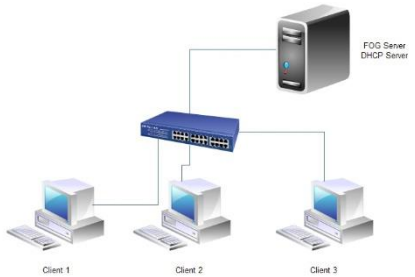
Nach der Registrierung weiterer PCs können diese ferngesteuert neu geklont werden.

Darüber hinaus bietet FOG die Möglichkeit, über sogenannte Snapins nachträglich Software und Einstellungen auf die Rechner zu verteilen. Hierfür sind Batch-Skripte und entsprechende Kenntnisse erforderlich.

Eine Installation des FOG-Servers in einer Laborübung würde den zeitlichen Rahmen von Präsenzfortbildungen sprengen. Eine detaillierte Anleitung zu FOG finden Sie unter:

https://schulnetz.alp.dillingen.de/materialien/Fog.pdf





MICROSOFT ENDPOINT MANAGER (GRUNDLAGEN)

MOBILE DEVICE MANAGEMENT (MDM)

Microsoft empfiehlt für die Verwaltung von Computern das Mobile-Device-Management-System „Microsoft Endpoint Manager“. Es ist Bestandteil der Cloud-Umgebung „Microsoft 365“.

Es bietet den Vorteil, dass an der Schule keine Serverinfrastruktur mehr betrieben werden muss. Dies bedeutet aber auch, dass eine performante, fehlerfrei konfigurierte Internetanbindung notwendig ist und Wartungsvorgänge teilweise sehr viel Verarbeitungszeit in Anspruch nehmen (mehrere Stunden, teilweise über Nacht). Insbesondere stark filternde DNS-Einstellungen können Probleme verursachen.

Da mit dem Endpoint Manager keine Images verwaltet, sondern einzelne Softwarepakete und Einstellungen verteilt werden, entfällt die Notwendigkeit, halbjährlich eine aktuelle Musterinstallation zu erstellen.

VORAUSSETZUNGEN

Für die Nutzung des Endpoint Manager sind Lizenzen erforderlich. Diese können als „Intune“-Lizenz pro Gerät gekauft oder gemietet werden oder als Bestandteil größerer Lösungen wie Microsoft 365 A3 zusammen mit Office- und Windows-Lizenzen gemietet werden.

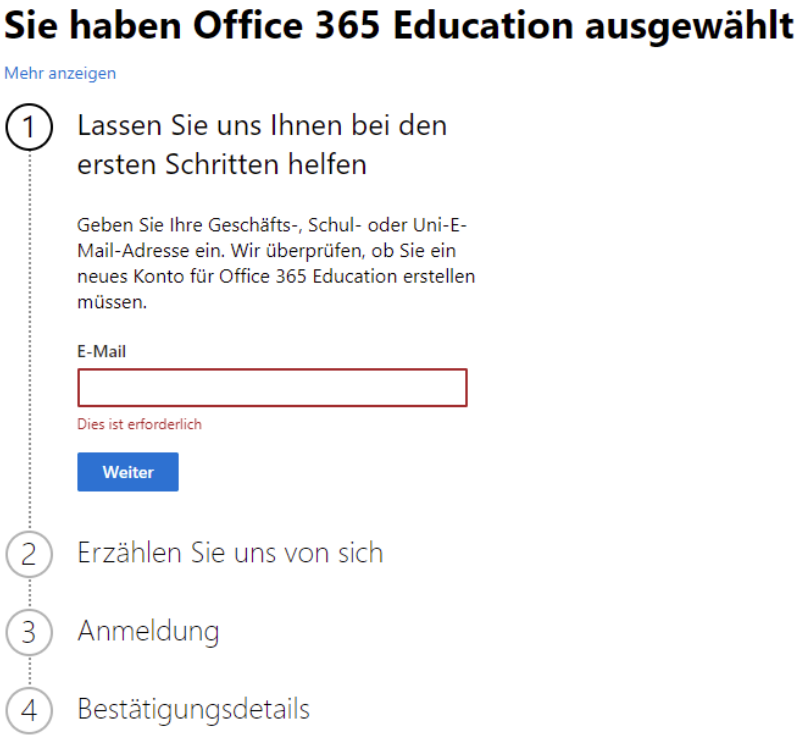
Darüber hinaus müssen alle PCs, die mit dem Endpoint Manager verwaltet werden sollen, über eine Windows-10/11-Pro-Lizenz (oder höher) verfügen. Diese sollte vorzugsweise in der Firmware des PC hinterlegt sein, was von allen großen PC-Herstellern angeboten wird.

TENANT EINRICHTEN

REGISTRIERUNG DES TENANTS

Um Windows-Geräte über Microsoft 365 zu verwalten, muss ein Tenant, quasi ein Hauptkonto für die gesamte Schule, angelegt werden. Dies wird in der Praxis meist durch einen externen Dienstleister unter Verwendung der Internet-Domain der Schule durchgeführt. Da die Eingabe der Domain sehr häufig notwendig ist, kann im Produktivbetrieb auch ein möglichst kurzer Domainname registriert werden. Eine nachträgliche Änderung des Domainnamens ist problematisch.

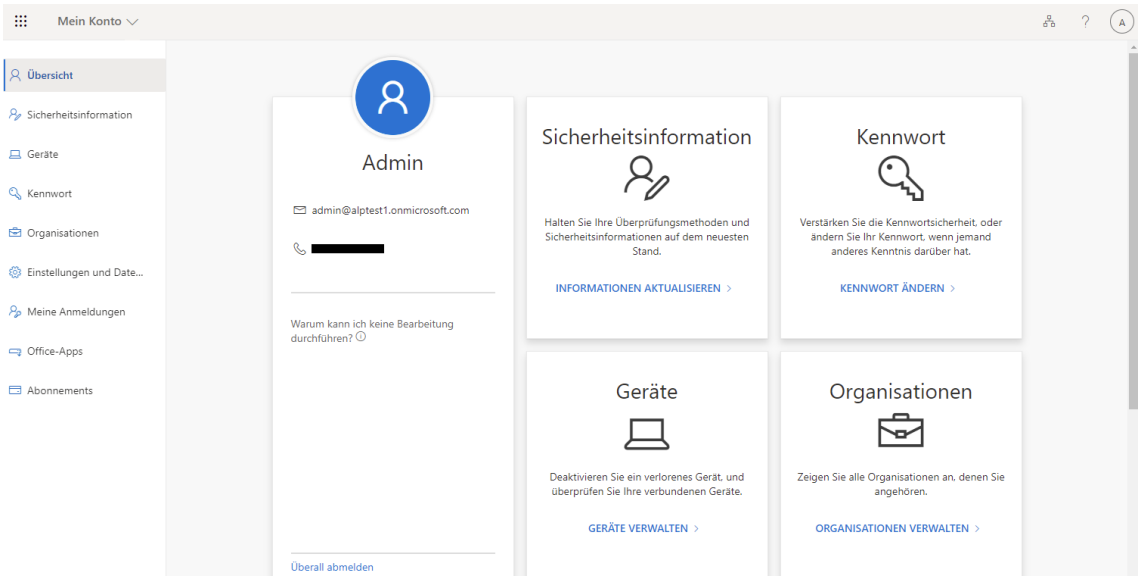
Unter der Adresse https://aka.ms/m365A3 kann innerhalb weniger Minuten ein kostenloser Tenant mit dem Funktionsumfang „A3“ für Testzwecke erstellt werden. Dazu sind eine Emailadresse und eine Telefon- oder Handynummer erforderlich. Es ist unwichtig, ob die Telefonnummer bereits bei anderen Accounts verwendet wurde.



Im Rahmen der Anmeldung muss eine Domain angelegt werden; für die Test-Tenants können beliebige noch verfügbare Bezeichnungen `*.onmicrosoft.com` registriert werden.

Als Benutzerkonto bietet sich „admin“ an. Passwörter müssen komplex sein; zu Übungszwecken eignet sich z. B. `Alp12345!`

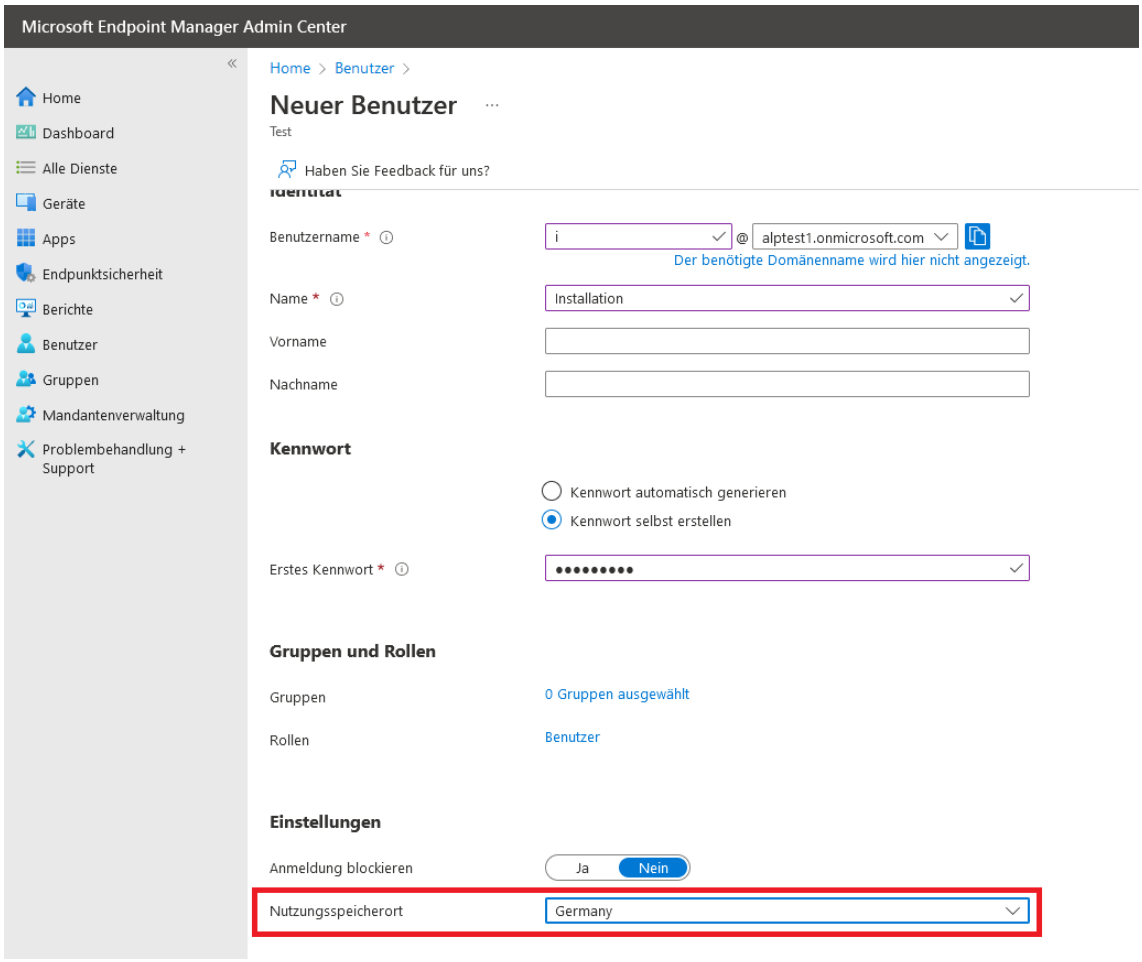
Nach Abschluss der Einrichtung steht unter https://myaccount.microsoft.com/ die folgende Übersicht des Tenants zur Verfügung:



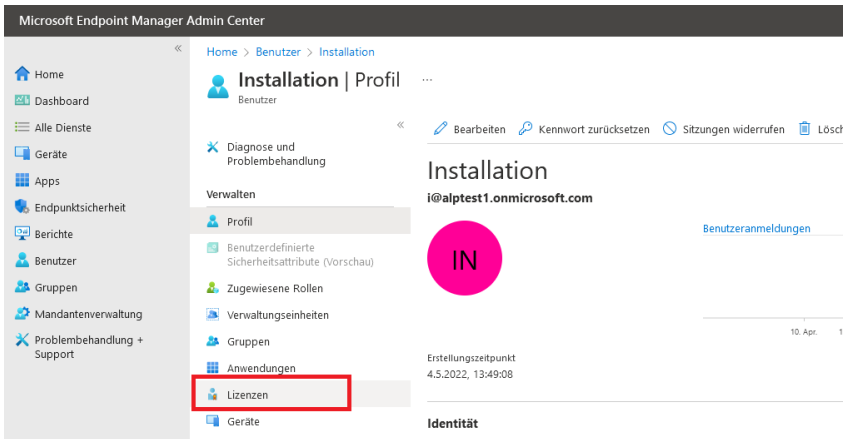
Die weitere Konfiguration des Tenants erfolgt im Wesentlichen über den Microsoft Endpoint Manager unter der Adresse https://endpoint.microsoft.com/.

BENUTZER EINRICHTEN

Neben dem bereits bestehenden Benutzer Admin sollte aus Sicherheitsgründen im Bereich „Benutzer“ mindestens ein weiteres Konto mit Administrationsrechten angelegt werden. Außerdem wird ein Konto zur Registrierung und Installation neuer PCs benötigt, das keine globalen Administrationsrechte haben sollte. Für dieses ist ein möglichst kurzer Benutzername vorteilhaft:

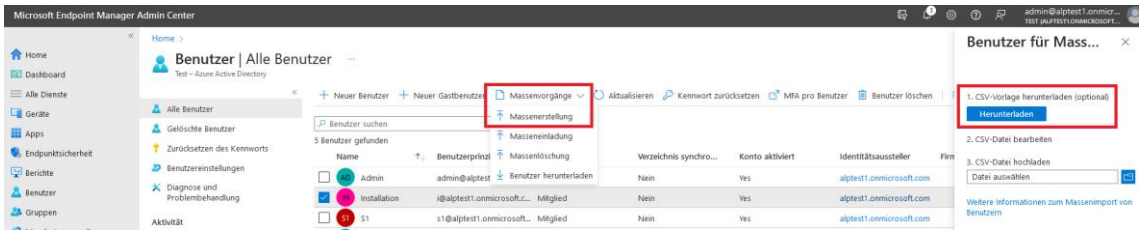


Die Rolle des „Globalen Administrators“ kann anschließend über die Schaltfläche „zugewiesene Rollen“ ausgewählt werden. Natürlich können die Rechte auch differenzierter vergeben werden. Dem Benutzer muss noch eine Lizenz zugewiesen werden:



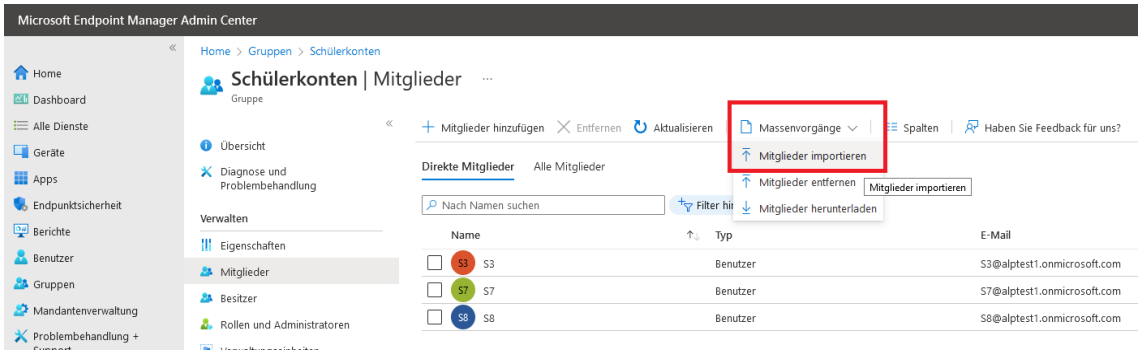
Für administrative Konten wie z. B. ein Installationskonto reicht auch eine Schülerlizenz aus.

In einem bereits bestehenden Tenant, der z. B. für den Betrieb von Microsoft Teams eingerichtet wurde, sind die Benutzer schon angelegt. In einem neuen Tenant können über die Funktion „Massenvorgänge“ mit geringem Aufwand mehrere Konten neu angelegt werden:

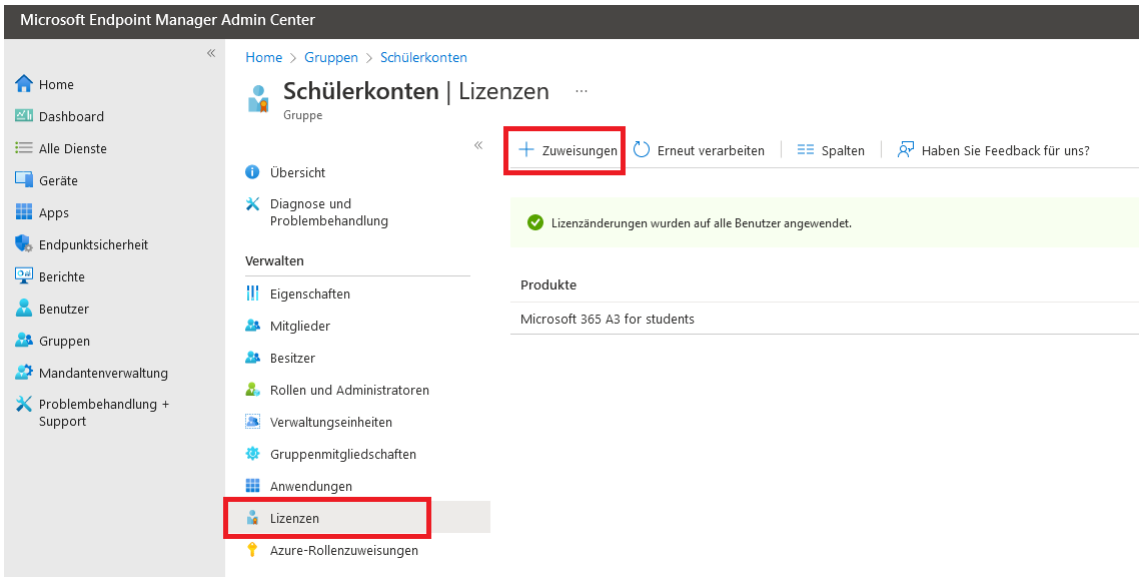


Eine Vorlagedatei im CSV-Format wird heruntergeladen und befüllt; hier sollte auch gleich der Nutzungsspeicherort „DE“ eingetragen werden.

Die Zuweisung der Lizenzen kann über eine Benutzergruppe erfolgen; diese erstellt man unter „Gruppen“. Auch hier gibt es eine Option zum Massenimport über eine CSV-Datei, in welche man lediglich die Emailadressen der gewünschten Mitglieder eintragen muss.



Abschließend kann die gewünschte Lizenz eingepflegt werden:

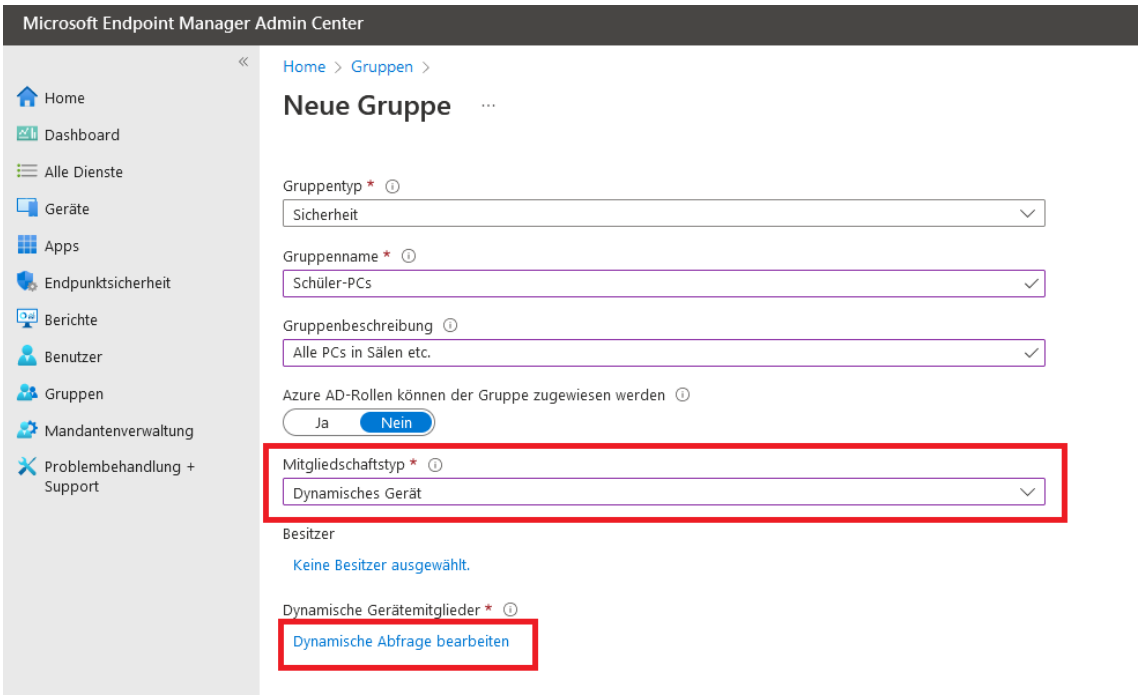


Es gibt Webdienste von kommerziellen Anbietern, die die Benutzer- und Lizenzverwaltung vereinfachen, insbesondere wenn Schüler zum Jahreswechsel in neue Klassen versetzt werden sollen und wenn Teams verwendet wird.

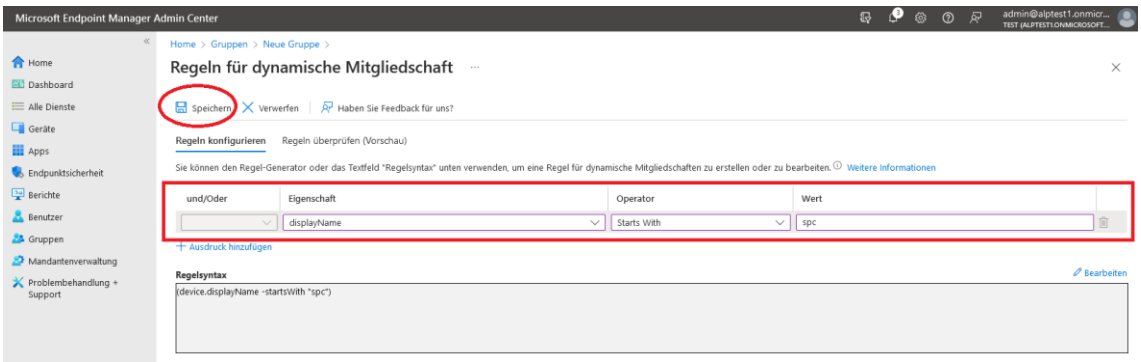
COMPUTERGRUPPEN EINRICHTEN

Um die an der Schule eingesetzten PCs sinnvoll verwalten zu können, sollten die Geräte in Gruppen eingeteilt werden. Denkbar sind z. B. Gruppen für Geräte, die von verschiedenen Personen genutzt werden (PCs in PC-Räumen, Klassenzimmern, Bibliothek…), Lehrerdienstgeräte, individuell zugeordnete Schülerleihgeräte etc.

Dazu wird im Bereich „Gruppen“ eine „neue Gruppe“ angelegt:



Sinnvoll ist die Einstellung „dynamisches Gerät“, welche eine manuelle Gruppenzuweisung erspart. Dazu wird eine „dynamische Abfrage“ hinzugefügt. Dies ermöglicht, die Geräte auf Basis des eingegebenen Computernamens automatisch der richtigen Gruppe zuzuordnen. Das Beispiel ordnet alle Rechner, deren Namen mit „spc“ beginnen, der Gruppe „Schüler-PCs“ zu.



Je nach Größe des Tenants kann die dynamische Zuweisung der Rechner zu Gruppen mehrere Stunden dauern.

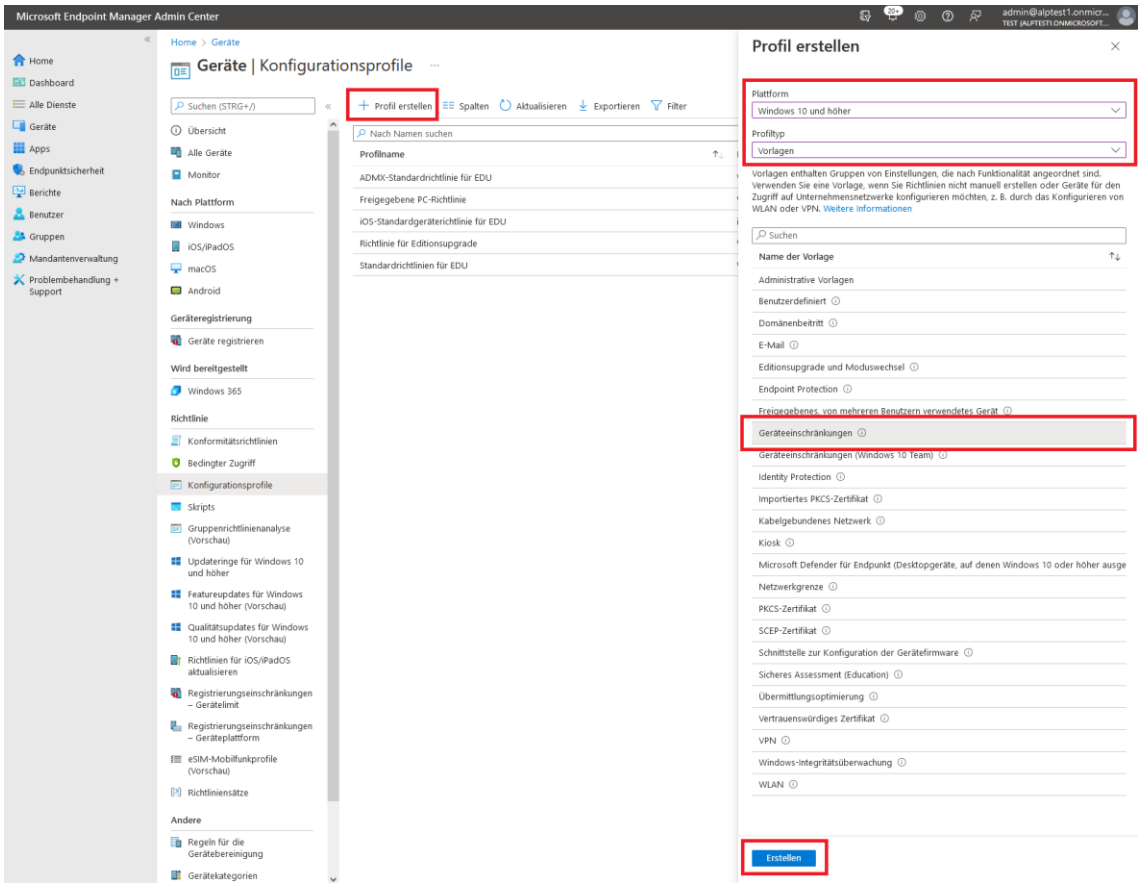
KONFIGURATIONSPROFILE VORBEREITEN

Im schulischen Umfeld macht es Sinn, gewisse Voreinstellungen für Windows zu treffen. Dies wurde bei „klassischen“ Installationsverfahren mittels Gruppenrichtlinien (GPO) umgesetzt. In Microsoft 365 werden stattdessen Konfigurationsprofile vorgegeben, die dann bestimmten Gerätegruppen zugeordnet werden. Diese werden im Bereich „Geräte – Konfigurationsprofile“ eingestellt. Für jede Einstellung wird über die Schaltfläche „Profil erstellen“ ein Eintrag generiert.

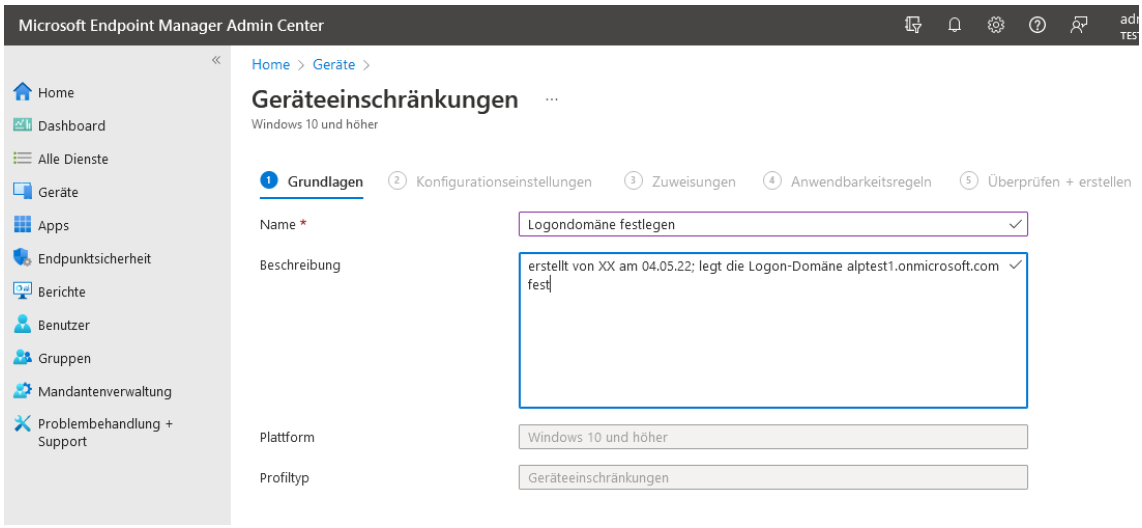
Als Beispiel soll die Logon-Domäne vorgegeben werden; dadurch wird den Nutzern erspart, den Domainteil ihrer Emailadresse bei der Anmeldung an den PCs einzutippen.

Nach einem Klick auf „Profil erstellen“ wird zunächst die Geräteplattform „Windows 10 und höher“ sowie der Profiltyp „Vorlagen“ gewählt. Dies ist bei allen im Folgenden genannten Profilen erforderlich.

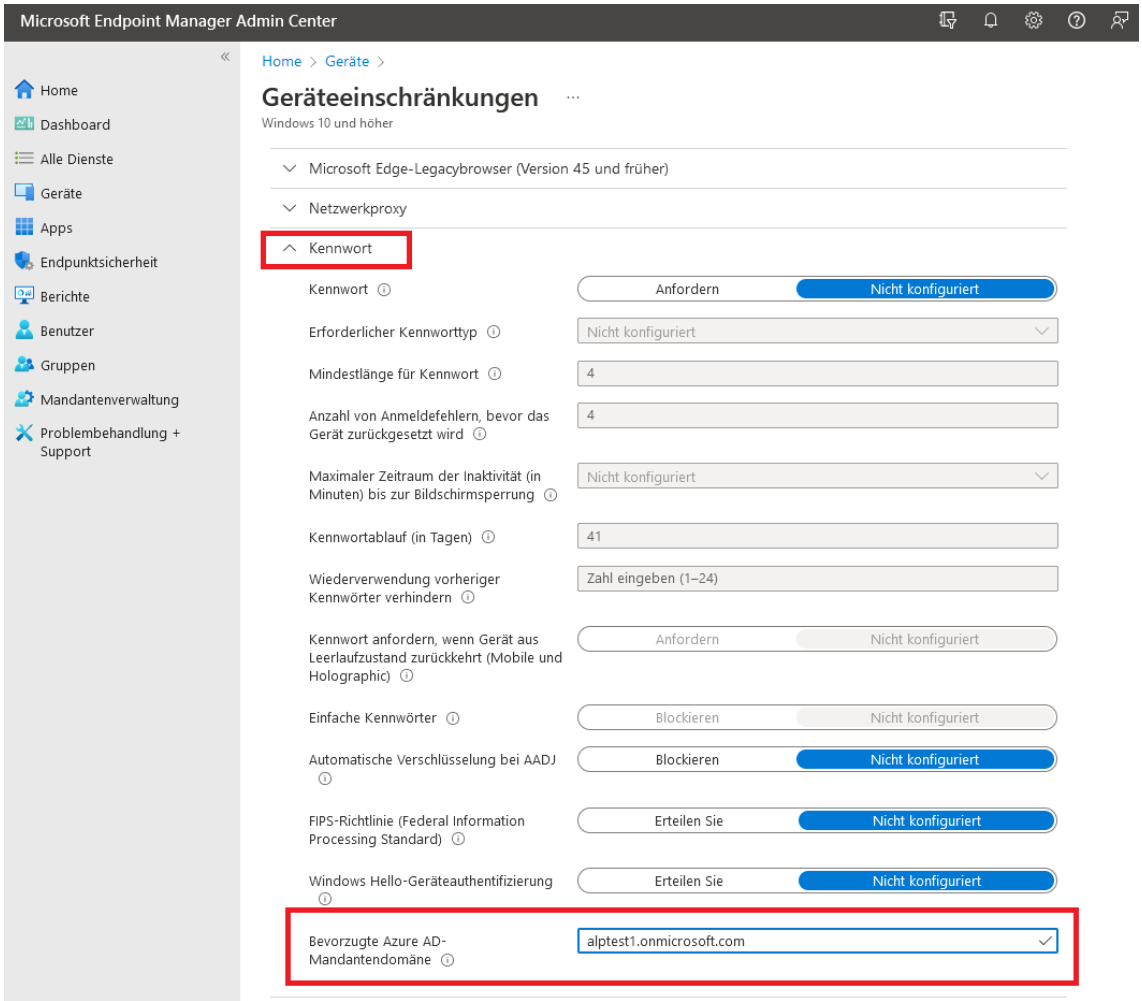
Für die Logon-Domäne wird nun der Bereich „Geräteeinschränkungen“ gewählt und mit „Erstellen“ bestätigt:



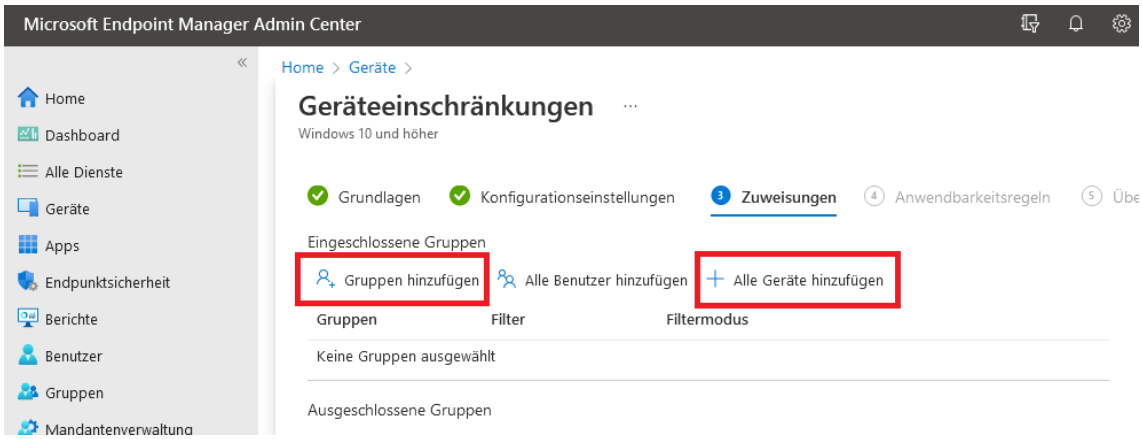
Wählen Sie einen aussagekräftigen Namen und geben Sie eine Beschreibung für das Profil ein:



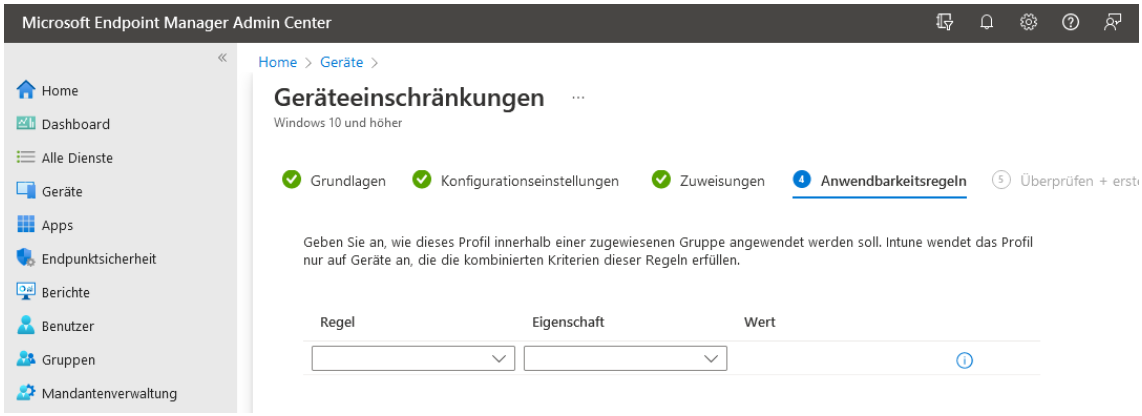
Erweitern Sie den Bereich „Kennwort“ und geben Sie unter „Bevorzugte Azure AD-Mandanten-domäne“ die Domäne Ihres Tenants ein:



Weisen Sie das neue Profil nun entweder allen Geräten oder nur einzelnen Gruppen zu:



Die folgende Abfrage „Anwendbarkeitsregeln“ kann leer bleiben:



Schließen Sie den Prozess auf der folgenden Seite mit „Erstellen“ ab.

In dieser Handreichung wird folgende Notation für die gerade vorgenommene Einstellung verwendet: *„Windows 10 / Vorlagen / Geräteeinschränkungen / Kennwort / Bevorzugte Azure AD-Mandantendomäne: Ihren Tenant-Domainnamen eintragen“*

Folgende weitere Konfigurationsprofile erscheinen sinnvoll:

- Biometrische Authentifizierung zulassen (z. B. Für Lehrerdienstgeräte):
  Windows 10 / Vorlagen / Identity Protection: Windows Hello aktivieren, Biometrische Authentifizierung zulassen
- WLAN vorkonfigurieren
  Windows 10 / Vorlagen / WLAN: WLAN-Typ i. d. R. Basis, SSID, Name und Sicherheitstyp eintragen
- Single Sign On für OneDrive aktivieren:
  Windows 10 / Vorlagen / Administrative Vorlagen - Computerkonfiguration – Onedrive: „Benutzer automatisch mit ihren Windows-Anmeldeinformationen bei der OneDrive-Synchronisierungs-App anmelden“ auf „Aktiviert“ setzen

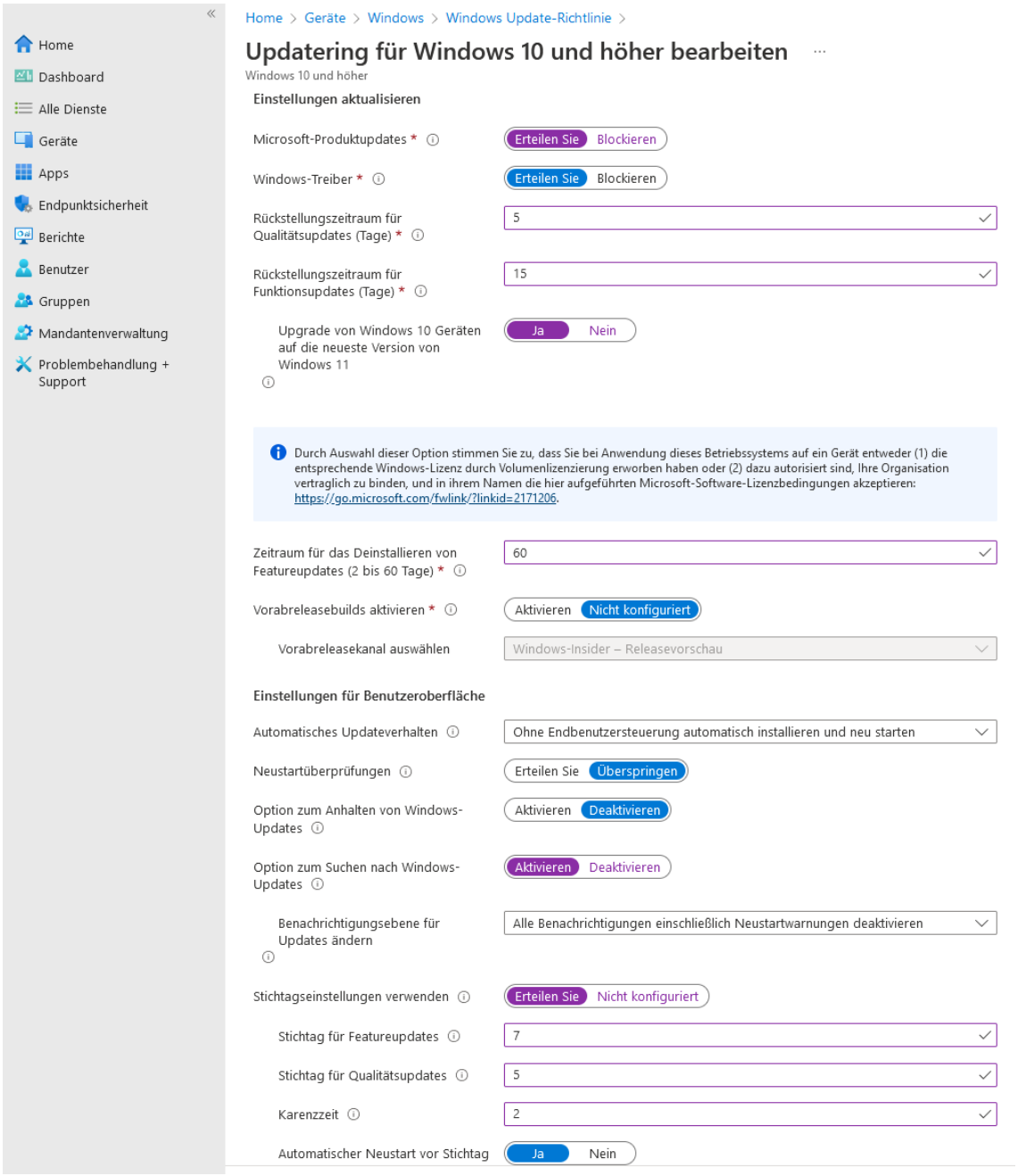
- Gastzugang aktivieren:
  Windows 10 / Vorlagen / Freigegebenes, von mehreren Benutzern verwendetes Gerät:

Modus für gemeinsame PC-Nutzung	Aktivieren
Gastkonto	guest,domain
Kontoverwaltung	Aktiviert
Kontolöschung	Bei Erreichen des Schwellenwerts für Speicherplatz und inaktive Konten
Schwellenwert (%) für das Starten von Löschungen	25
Schwellenwert (%) für das Beenden von Löschungen	35
Schwellenwert für inaktive Konten	60
Lokaler Speicher	Aktiviert
Energieverwaltungsrichtlinien	Aktiviert
Timeout für Energiesparmodus (in Sekunden)	3600
Anmeldung bei PC-Reaktivierung	Aktiviert
Startzeitpunkt für Wartung (in Minuten ab Mitternacht)	
Education-Richtlinien	Aktiviert

  Ist der Gastzugang aktiviert, kann man sich am PC ohne Zugangsdaten anmelden, hat dann allerdings keine Office-Lizenz und keinen Zugriff auf z.B. in OneDrive gespeicherte Daten. Alle anderen Programme und insbesondere der Internetzugang sind voll funktionsfähig.

WINDOWS UPDATE-EINSTELLUNGEN

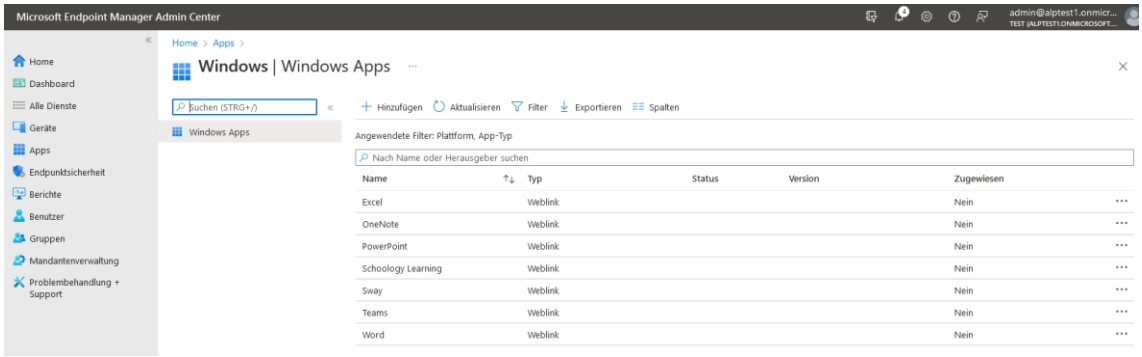
Im Bereich „Geräte – Windows – Updateringe für Windows 10 und höher“ wird das Verhalten von Windows Update konfiguriert. Ein wesentlicher Punkt ist derzeit das Upgrade von Windows 10-Geräten auf Windows 11. Der folgende Screenshot zeigt eine Beispielkonfiguration, in der u. A. das Upgrade auf Windows 11 erlaubt wird:



SOFTWAREPAKETE VORBEREITEN

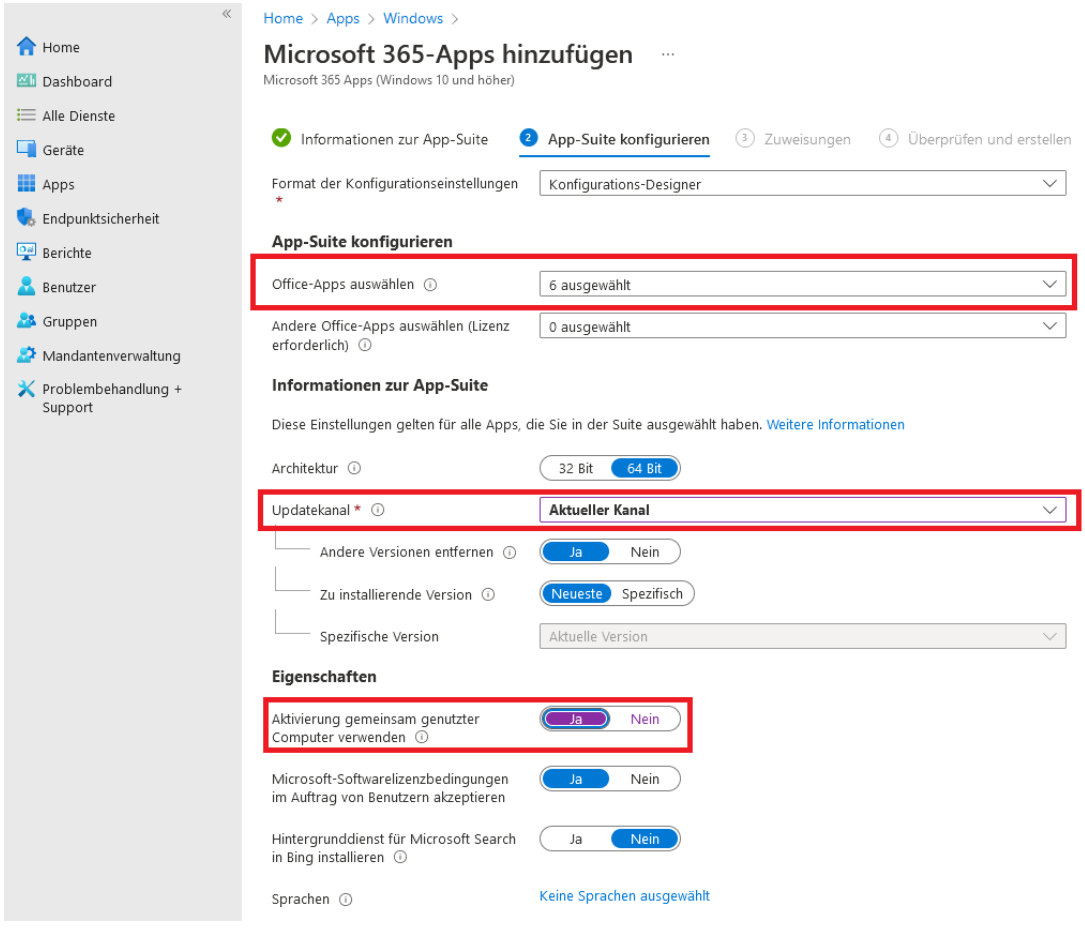
STANDARD-LINKS LÖSCHEN

Im Bereich „Apps – Windows“ sind bereits diverse Weblinks eingepflegt, welche mittels „…“ gelöscht werden können, wenn die Schule über bessere Lizenzen als A1 verfügt:



MICROSOFT OFFICE

Softwarepakete werden im Bereich „Apps – Windows“ bereitgestellt. Besonders bequem zu installieren ist Microsoft Office. Über „Hinzufügen – Microsoft 365 Apps, Windows 10 und höher“ erreicht man einen Konfigurationsbildschirm, in dem man die gewünschten Office-Programme sowie den Update-Kanal wählen kann. Die Option „Aktivierung gemeinsam genutzter Computer“ ist wichtig, da sonst auf gemeinsam genutzten Geräten eine der fünf persönlichen Office-Aktivierungen des Benutzers verwendet wird.



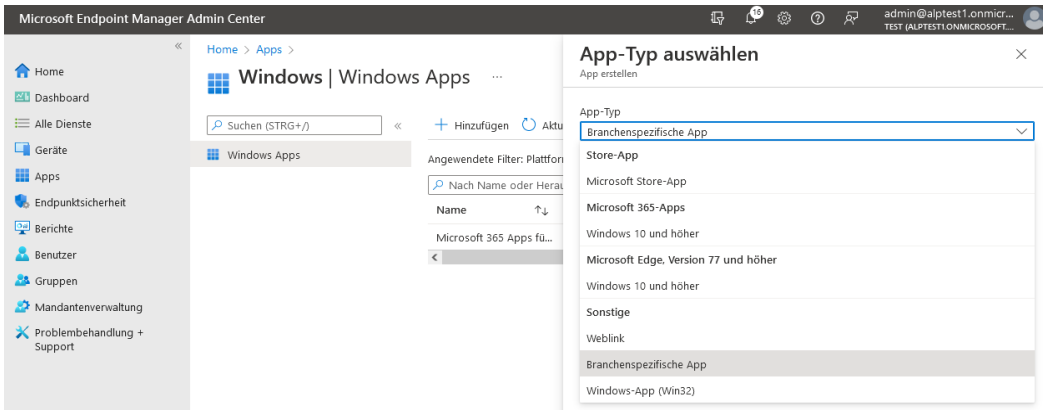
Die Software wird nun vom Client abgerufen; je nach Alter der Installation kann ein automatischer Abruf bis zu 8 Stunden dauern. Bei einem Neustart des Geräts wird automatisch auf ausstehende Installationen geprüft.

MICROSOFT STORE APPS

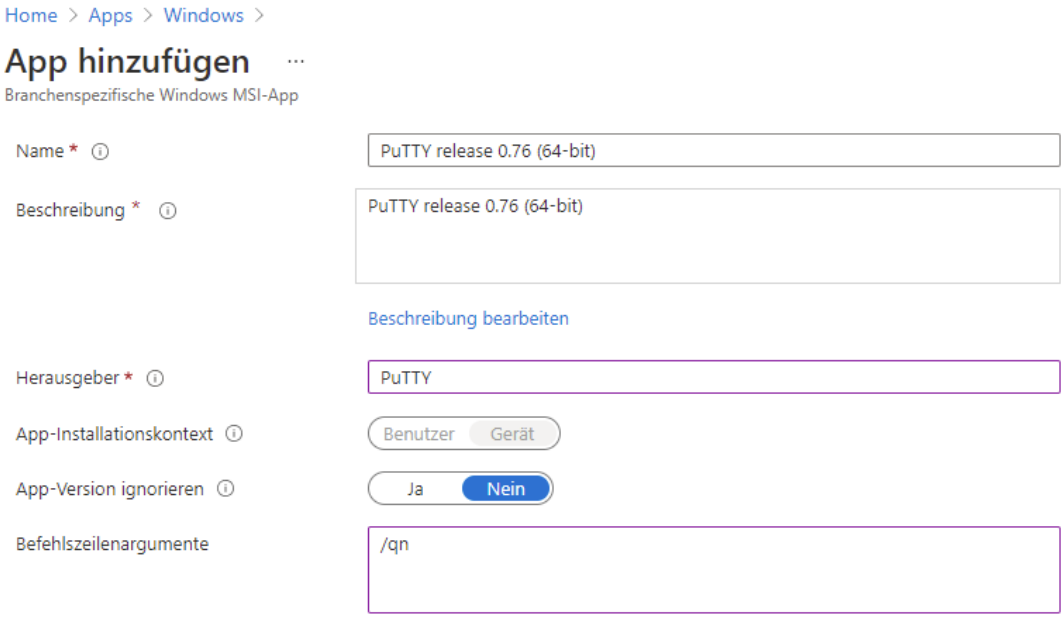
Microsoft überarbeitet derzeit die Softwareverteilung von Apps aus dem Microsoft Store. Noch im Jahr 2022 sollen solche Apps über den neuen Windows-Paketmanager „winget“ verwaltet werden, so dass eine Einarbeitung in die Verteilung aktuell nicht lohnenswert erscheint.

MSI-PAKETE

Die Verteilung von Software, die vom Hersteller in Form eines MSI-Pakets zum Download angeboten wird, ist einfach. Nach dem Download wird über den Endpoint Manager per „Apps – Windows – Hinzufügen“ eine „Branchenspezifische App“ definiert. Als App-Paketdatei wird das MSI-Paket hochgeladen:



Der Endpoint Manager weiß, wie ein MSI-Paket auf dem Endgerät installiert wird, sodass kein Installationsbefehl angegeben werden muss. Damit die Installation aber ohne Rückfragen durchläuft, sollte im Feld „Befehlszeilenargumente“ der Parameter `/qn` angegeben werden:



Bei der Zuweisung der App zu Geräte- oder Benutzergruppen gibt es folgende Möglichkeiten:

- **Erforderlich / Required**
  Die App wird auf den entsprechenden Geräten verpflichtend installiert. Dies ist die übliche Auswahl für Schulen.
- **Für registrierte Geräte verfügbar**
  Benutzer können selbst entscheiden, ob diese App installiert werden soll oder nicht. Dazu muss die „Unternehmensportal-App“ eingerichtet werden. Da diese Art der Softwareverteilung an Schulen normalerweise keine Rolle spielt, geht dieses Dokument nicht näher darauf ein.

Für viele beliebte Programme wie z. B. Firefox findet man fertige MSI-Pakete im Internet, auch wenn das MSI-Paket nicht direkt auf der Startseite zum Download angeboten wird.

DRUCKER VERBINDEN

DRUCKER ÜBER IP-ADRESSE EINBINDEN

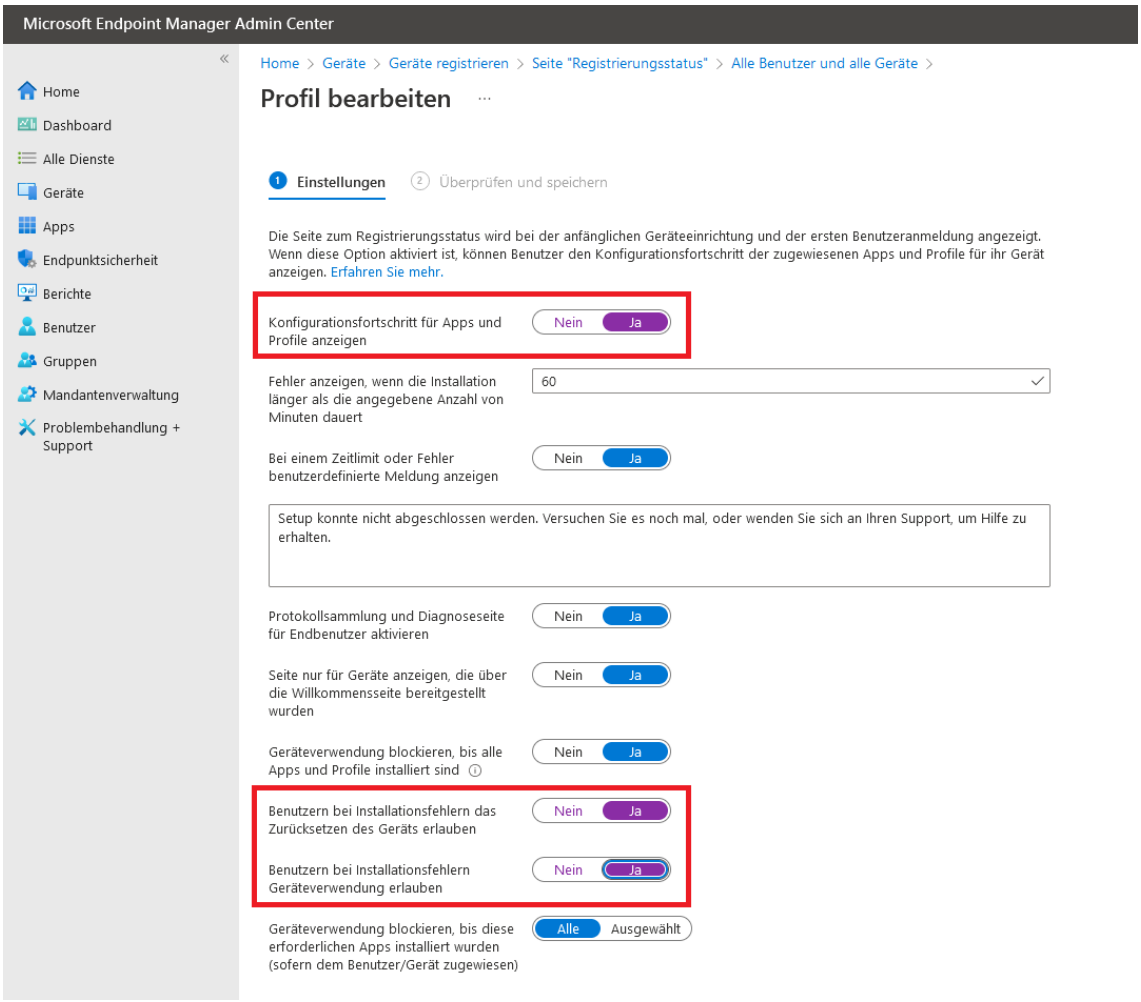
Im Endpoint Manager wird über Geräte -> Konfigurationsprofile -> Plattform Windows 10 / Typ Vorlagen -> Geräteeinschränkungen ein Konfigurationsprofil angelegt. Darin kann man im Abschnitt „Drucker“ die IP-Adressen der gewünschten Drucker angeben. Wenn der Drucker von Windows unterstützt wird, erscheint er nach der Zuweisung des Konfigurationsprofils an eine Geräte- oder Benutzergruppe auf den entsprechenden Endgeräten. Ein Treiber wird nicht benötigt. Da dieses einfache Verfahren auf IPP (Internet Printing Protocol) basiert, funktioniert die Verteilung leider nicht mit jedem Drucker. Dies sollte bei der Beschaffung neuer Geräte berücksichtigt werden.

Die Einbindung von Druckern, die einen separaten Treiber benötigen, ist aufwändiger und im letzten Kapitel dieser Handreichung beschrieben.

RECHNER IN DEN TENANT AUFNEHMEN

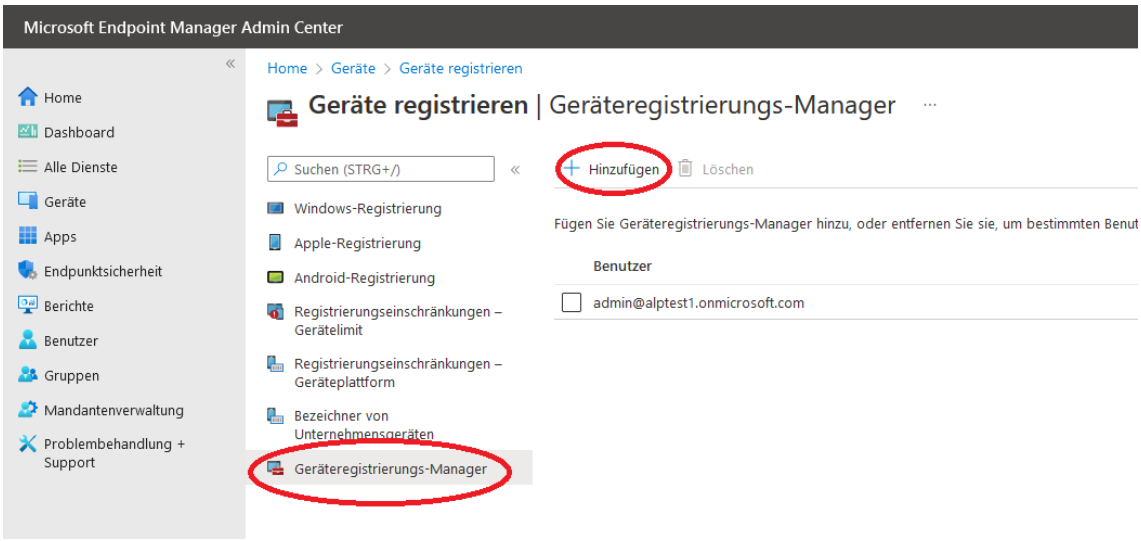
REGISTRIERUNG VON CLIENTGERÄTEN VORBEREITEN

Vor der Aufnahme von Geräten ist es sinnvoll, die Registrierungsstatus-Seite unter „Geräte – Geräte registrieren – Seite ‚Registrierungsstatus'" zu konfigurieren. Ist diese eingerichtet, werden die Konfigurationsschritte während der Aufnahme des Clients ausgegeben, was die Installation der Clients übersichtlicher macht. Ist die Seite nicht konfiguriert, werden die Installationsschritte ohne grafische Anzeige im Hintergrund durchgeführt, was Fehleranalysen erschwert. Die markierten Einstellungen werden empfohlen, auch, um bei Verzögerungen das Gerät dennoch schon benutzbar zu machen:



GERÄTEREGISTRIERUNGSKONTO FESTLEGEN

Ein oder mehrere Benutzer müssen berechtigt werden, neue Rechner in den Tenant aufnehmen zu dürfen. Im Bereich „Geräte – Geräte registrieren – Geräteregistrierungs-Manager“ muss mindestens ein Benutzerkonto als Geräteregistrierungs-Manager hinzugefügt werden:

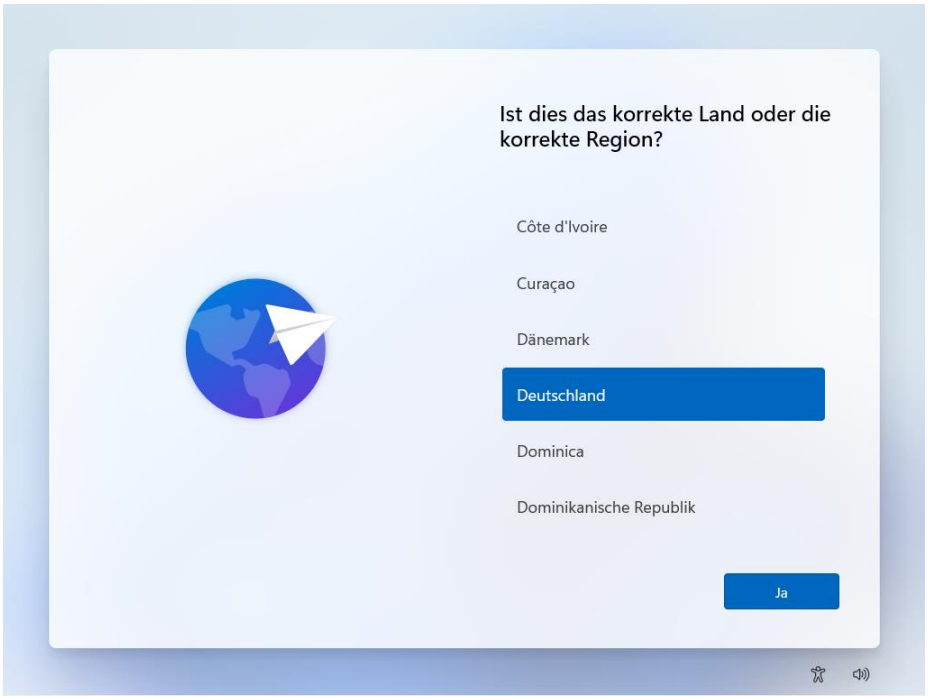


Solange das verwendete Konto keine weitergehenden Administrationsrechte hat, kann die Geräteregistrierung

GERÄTE AUFNEHMEN

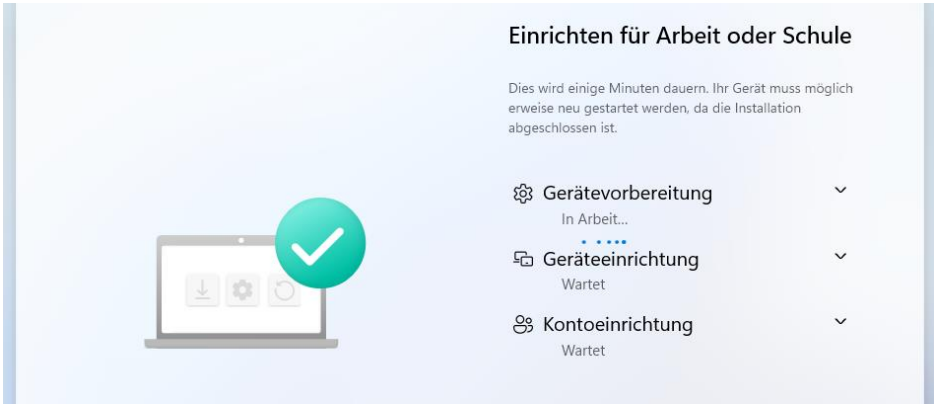
Damit nur Benutzer mit der Rolle „Geräteregistrierungs-Manager“ neue Geräte mit dem Tenant verbinden können (und nicht etwa Schüler ihre Privatgeräte), muss im Endpoint Manager unter Geräte / Geräte registrieren / Registrierungseinschränkungen-Geräteplattform das Standard-Profil für alle Benutzer angepasst werden:

Die Aufnahme eines neuen Geräts beginnt mit der OOBE (Out-of-the-box-experience), die entweder nach einer Neuinstallation des Betriebssystems oder der Inbetriebnahme neu angelieferter Rechner automatisch durchlaufen wird. Bereits vorhandene Rechner sollten zurückgesetzt oder neu installiert werden. Ist dies nicht möglich (z.B. bei schon im Umlauf befindlichen Lehrerdienstgeräten), kann ein Gerät auch über die Systemsteuerung / „Auf Arbeits- oder Schulkonto zugreifen“ / „Nur bei Geräteverwaltung registrieren“ beim Endpoint Manager registriert werden.



Nach der Abfrage von Region, Tastatureinstellungen und ggf. der Verbindung mit einem WLAN kann ab Windows 11 bereits ein Rechnername vergeben werden. Vergeben Sie einen Namen, der einer Computergruppe zugeordnet werden kann (vgl. Kapitel 5, „Computergruppen“).

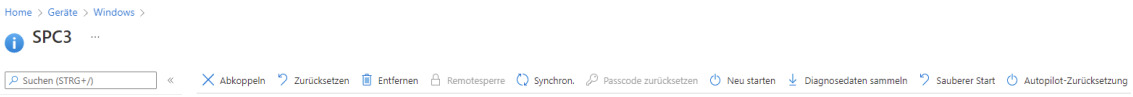
Wählen Sie die Option „Für Arbeit oder Schule/Uni einrichten“ und melden Sie sich mit dem zur Registrierung berechtigten Konto am Rechner an. Der Rechner kontaktiert nun den Tenant, um die relevanten Einstellungen und Softwarepakete zu beziehen. Dies wird, falls Sie die Registrierungsseite wie am Anfang des Kapitels konfiguriert haben, auch angezeigt:



Sobald der Prozess abgeschlossen ist, kann sich ein beliebiger Nutzer am Rechner anmelden. Zu beachten ist, dass die meisten konfigurierten Einstellungen (Software, Profile) erst nach längerer Wartezeit vom Endgerät übernommen werden.

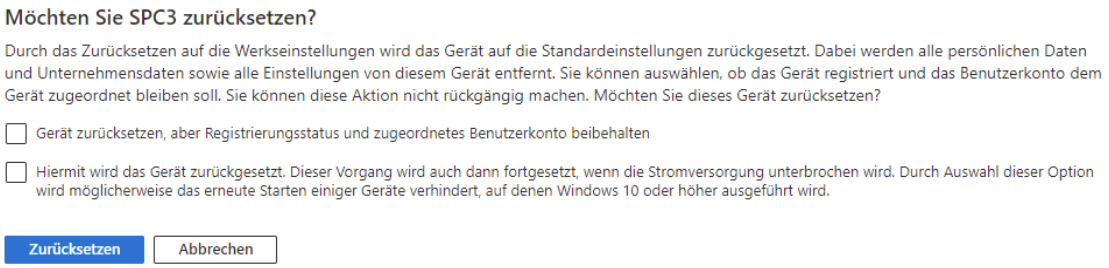
GERÄTE ZURÜCKSETZEN ODER NEU INSTALLIEREN

Schülerleih- und Lehrerdienstgeräte müssen zurückgesetzt werden, bevor sie an den nächsten Nutzer ausgegeben werden. Der Endpoint Manager bietet dazu verschiedene Möglichkeiten, die nach einem Klick auf den Gerätenamen unter Geräte / Windows angeboten werden:



Von Bedeutung sind dabei „Zurücksetzen“ und „Autopilot-Zurücksetzung“.

ZURÜCKSETZEN



Der erste Haken wird nicht gewählt, da die Benutzerdaten ja gerade gelöscht werden sollen. Die zweite Option sollte normalerweise auch nicht gesetzt werden, da bei einer bereits beschädigten Windows-Installation auf dem Gerät der PC in einer Endlos-Startschleife festhängen kann. Sie kann bei verlorenen oder gestohlenen Geräten verwendet werden.

Das Zurücksetzen ohne die beiden Häkchen entspricht dem Zurücksetzen am Gerät über das Startmenü / „Diesen PC zurücksetzen“.

Während der Rücksetzung wird Windows vollständig neu installiert. Nach dem Zurücksetzen ist das Gerät nicht mehr mit dem Endpoint Manager verbunden und muss durch Anmelden mit einem Geräteregistrierungsmanager neu verknüpft werden.
Eine eventuelle Autopilot-Registrierung (vgl. folgendes Kapitel) wird durch die Rücksetzung nicht aufgehoben!

AUTOPILOT-ZURÜCKSETZUNG

Diese Option ist entgegen der Bezeichnung auch für Nicht-Autopilot-Geräte verfügbar. Sie löst keine Windows-Neuinstallation aus, sondern entfernt nur alle Benutzerdaten und installierten Programme. Sie eignet sich besonders für noch funktionierende Schülerleih- oder Lehrerdienstgeräte, die schnell zurückgesetzt werden sollen, um an den nächsten Benutzer ausgegeben zu werden.

Soll die Autopilot-Zurücksetzung auch direkt vom Gerät aus möglich sein, muss ein Konfigurationsprofil „Windows 10 / Vorlagen / Geräteeinschränkungen / Allgemein / Autopilot Reset“ angelegt werden. Anschließend kann vom Sperrbildschirm aus mit der Tastenkombination Strg + Windows + R und Eingabe eines Benutzers mit Administratorrechten das Gerät zurückgesetzt werden.

VORSICHT

Wegen eines bekannten Fehlers in Windows 10 und 11 wird mit Stand Mai 2022 ein Teil der Benutzerdaten nicht gelöscht, sondern ist mit Administratorrechten nach der Zurücksetzung im Ordner Windows.old\Users zu finden. Microsoft hat angekündigt, diesen Fehler zu beheben.

MICROSOFT ENDPOINT MANAGER (VERTIEFT)

AUTOPILOT

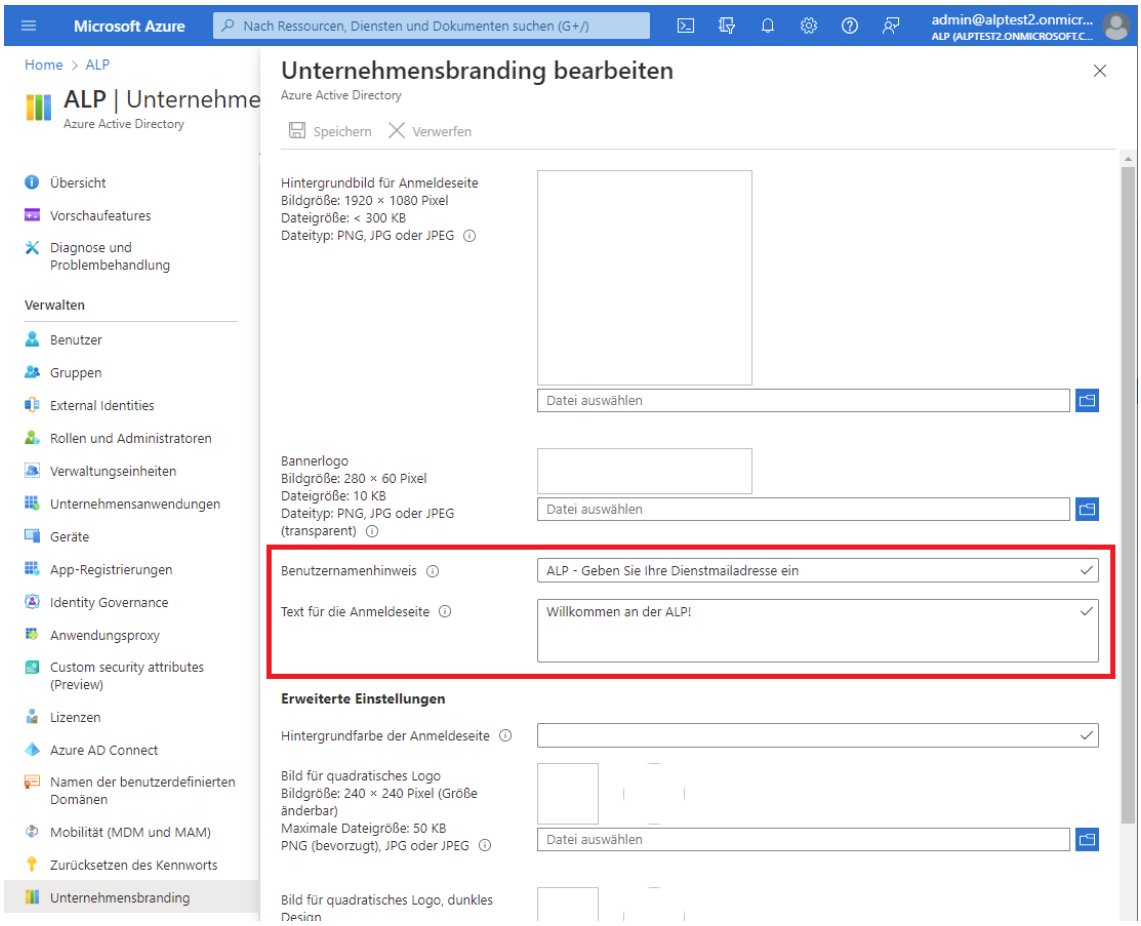
FUNKTION UND TECHNISCHE VORAUSSETZUNGEN

Die Autopilot-Funktion vereinfacht das im letzten Kapitel beschriebene Verfahren der Aufnahme von Rechnern in den Tenant bedeutend. Im Optimalfall ist für die Einrichtung neuer Rechner oder Reparaturinstallationen kein Eingreifen des Systembetreuers mehr erforderlich.

Für Autopilot sind Geräte mit einem Trusted Platform Module in (mindestens) der Version 2.0 erforderlich (TPM 2.0). Virtuelle PCs, die ein TPM nur simulieren können, werden von Autopilot nicht akzeptiert. Außerdem muss „UEFI Secure Boot“ aktiviert sein.

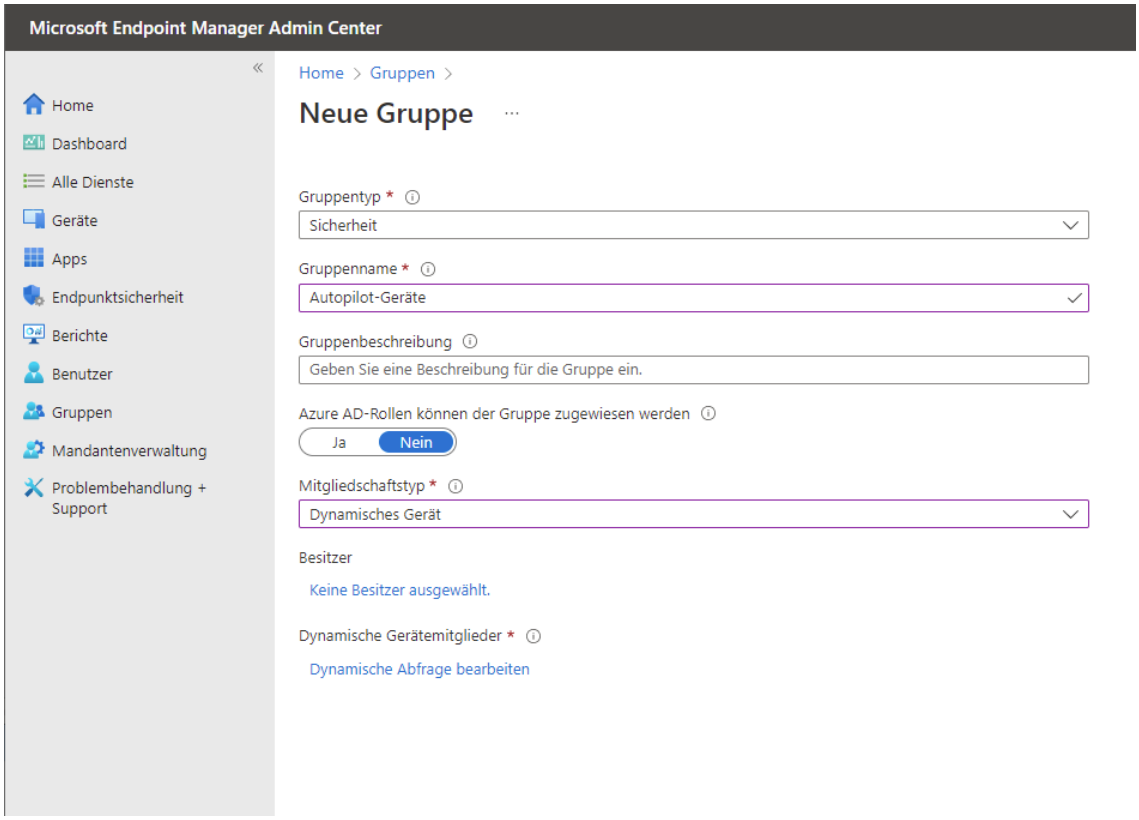
EINRICHTUNG VON AUTOPILOT

Um die volle Funktionsfähigkeit von Autopilot zu gewährleisten, muss im Azure Active Directory (https://portal.azure.com) das „Unternehmensbranding“ konfiguriert werden. Dabei genügt es schon, die markierten Textfelder auszufüllen:



Das Azure Active Directory kann nun wieder geschlossen werden, der Rest des Setups geschieht im Endpoint Manager.

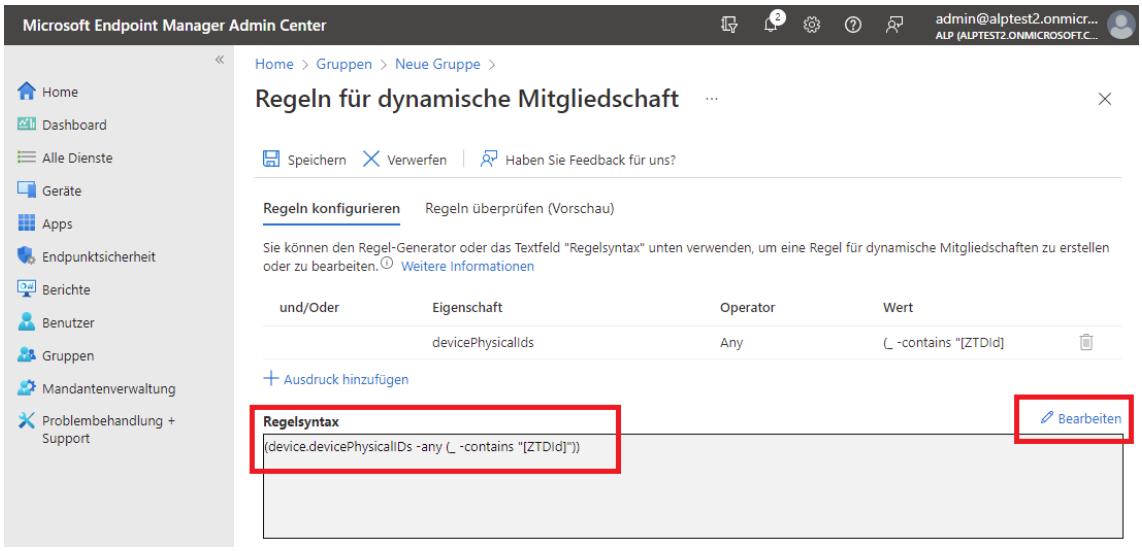
Auf der Endpoint-Manager-Seite „Gruppen“ muss eine neue Gruppe für die Autopilot-Geräte erstellt werden. Der Mitgliedschaftstyp muss auf „Dynamisches Gerät“ gesetzt werden:



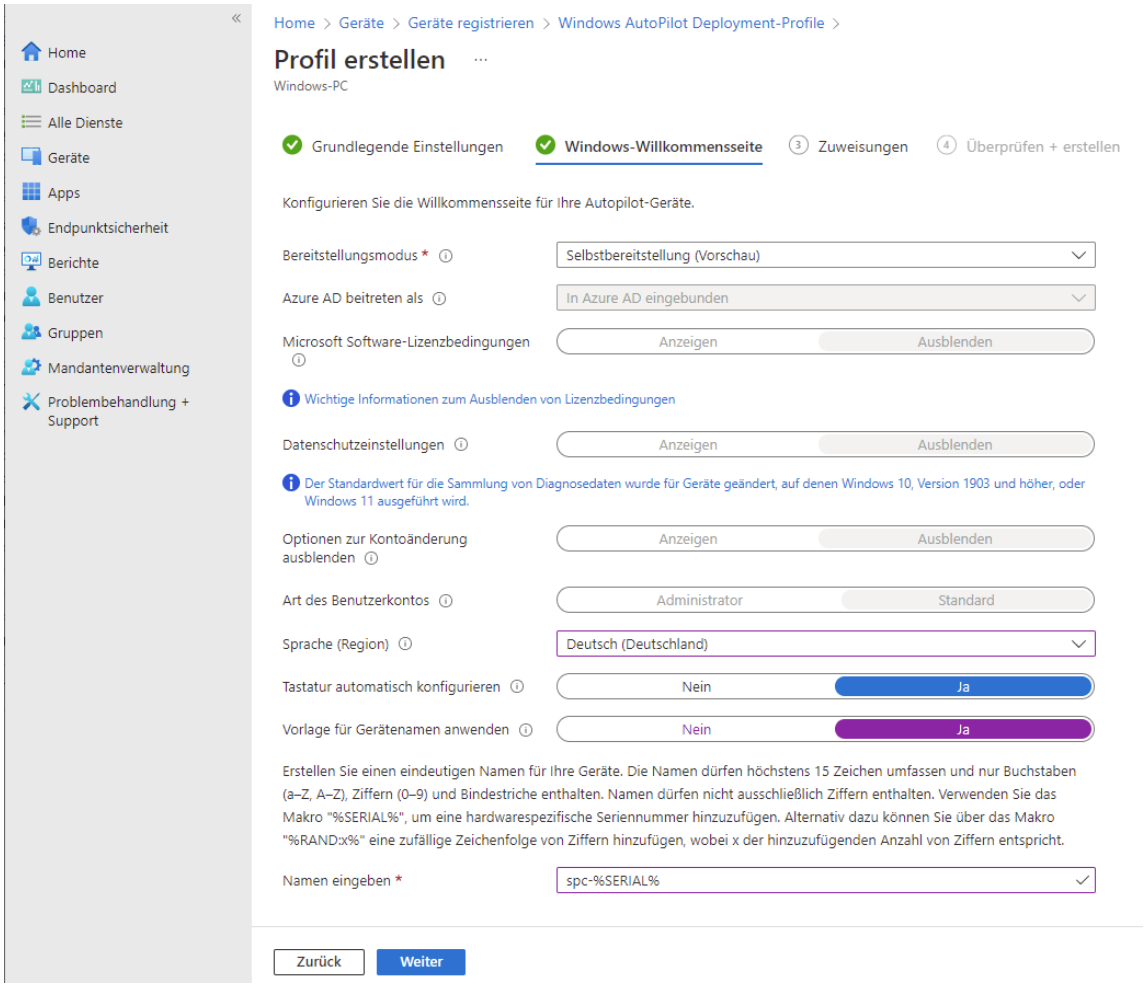
Anschließend wird eine dynamische Abfrage erstellt. Um Fehler zu vermeiden, sollte der Ausdruck

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

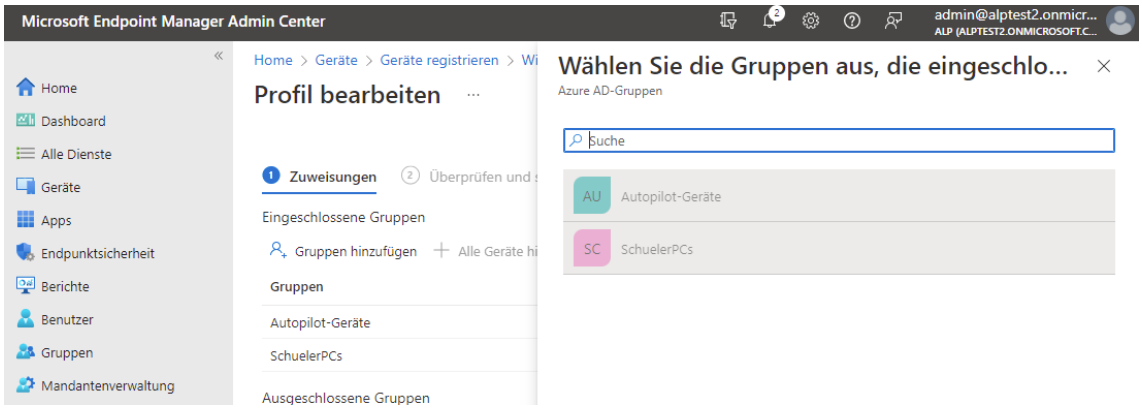
kopiert und in das Feld „Regelsyntax“ eingefügt werden:



Im nächsten Schritt werden im Bereich „Geräte – Geräte registrieren – Bereitstellungsprofile“ zwei neue Profile für „Windows-PC“ eingerichtet. Mit dem ersten Profil und den folgenden Einstellungen werden Autopilot-Geräte erfasst, die per PowerShell-Skript (s. u.) registriert werden. Als Computernamen wird spc-%SERIAL% angegeben; dadurch erhalten die Rechner einen Namen beginnend mit spc-, der sie automatisch als schuleigene Computer zuordnet, und ihre Seriennummer, um sie leichter zu identifizieren.



Das Profil wird der vorher erstellten Gruppe „Autopilot-Geräte“ sowie der Gruppe „SchuelerPCs“ zugeordnet:



Damit sind die Vorarbeiten für Autopilot abgeschlossen.

GERÄTE IN AUTOPILOT AUFNEHMEN

Geräte können auf mehrere Arten in Autopilot aufgenommen werden.

1. Aufnahme durch den Lieferanten: Der Hersteller bzw. CSP (Cloud Solution Provider) registriert das Gerät im Tenant der Schule. Dafür benötigt er nur die Tenant-Bezeichnung der Schule. Bei der Inbetriebnahme installieren sich die PCs selbsttätig.

2. Vorabdaten des Lieferanten: Der Hersteller bzw. CSP (Cloud Solution Provider) schickt dem Systembetreuer eine CSV-Datei zum Import in den Tenant zu. Dieser importiert die Daten über die entsprechende Funktion im Bereich Geräte / Geräte registrieren / Geräte; auch hier installieren sich die PCs anschließend selbsttätig.

3. Registrierung mittels OOBE: Die Out-of-box-experience wird normal durchlaufen (Anmeldung als Geräteregistrierungs-Manager) und dabei ein Computername vergeben, der mit „spc“ beginnt. Aufgrund des im Beispiel konfigurierten Bereitstellungsprofils wird der Rechner automatisch als Autopilot-Gerät erfasst. Bei der ersten Einrichtung ist dies noch keine Arbeitsersparnis, doch das Gerät kann danach leichter administriert werden (z. B. Neuinstallation, Zurücksetzen…).

4. Registrierung mittels PowerShell-Skript: Während die Rechner die OOBE durchlaufen und mit dem Internet verbunden sind (Ethernet oder WLAN), wird mit der Tastenkombination Shift + F10 eine Eingabeaufforderung geöffnet.

   Variante A: Ein vorbereiteter USB-Stick mit dem „AutopilotHashErmittlungsSkript“ wird angeschlossen und die Skriptdatei „StartAutopilotHashErmittlung.cmd“ wird gestartet. Dadurch wird eine Zeile mit dem Hashwert des Computers auf dem Stick an den Anfang (!) der Datei computers.csv geschrieben. Dieser Vorgang kann bei weiteren Computern wiederholt werden. Die Datei computers.csv entspricht der Datei des Lieferanten aus Schritt 2 und wird entsprechend importiert.

   Variante B: Folgende Befehle eingegeben (ggf. mit „Tab-Vervollständigung“), Rückfragen mit „j“ beantworten:

   ```
   powershell
   Set-ExecutionPolicy bypass
   Install-Script Get-WindowsAutoPilotInfo
   Get-WindowsAutoPilotInfo.ps1 -Online
   ```

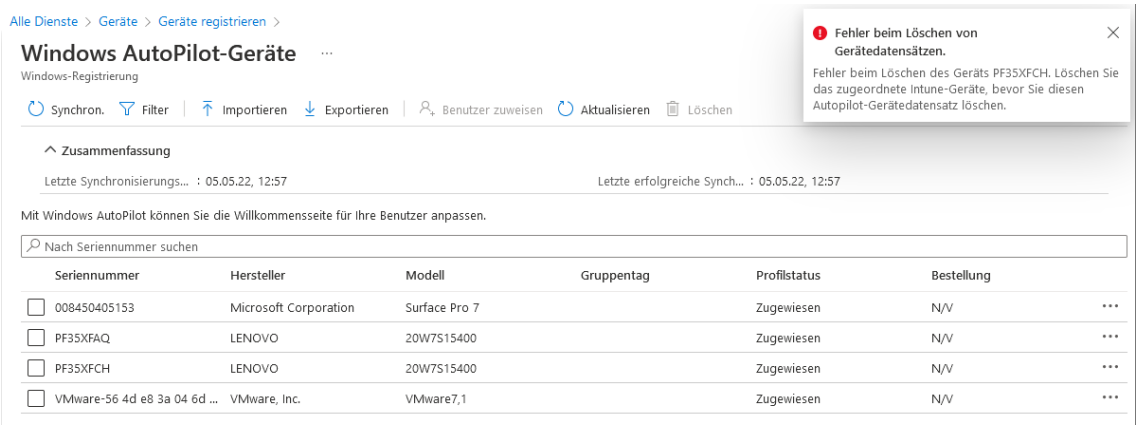
   Das Skript registriert den Rechner beim Tenant und übermittelt die Hardware-ID. Dazu wird das Login eines Geräteregistrierungskonto verlangt. Die Aufnahme kann einige Zeit in Anspruch nehmen. War der Vorgang erfolgreich, kann der Rechner mit `shutdown -r -t 900` neu gestartet werden. Durch die Verzögerung von 900 Sekunden wird die Wahrscheinlichkeit erhöht, dass beim Neustart die Autopilot-Information bereits von den Microsoft-Servern verarbeitet wurde.

   Das neue Gerät sollte nun im Bereich „Windows Autopilot-Geräte“ angezeigt werden.

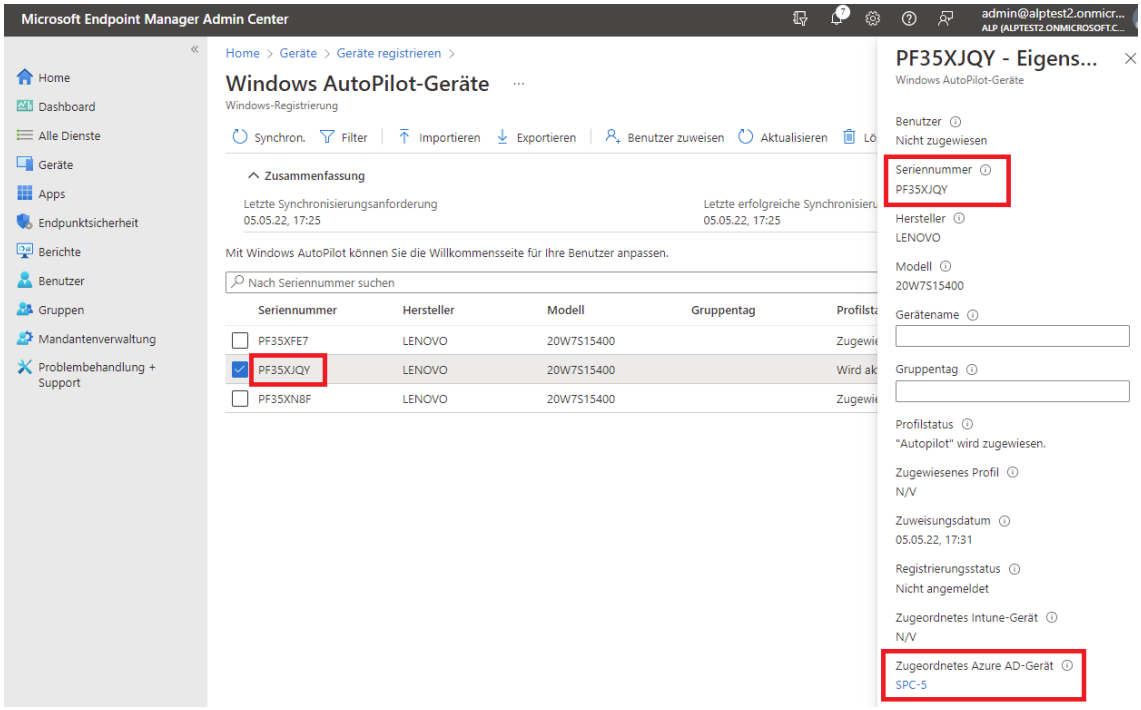
AUTOPILOT-GERÄTE ENTFERNEN

Mit Autopilot verbundene Geräte sind fest an ihren Tenant gebunden und können ausschließlich von einem Administrator oder dem Microsoft-Support daraus wieder entfernt werden. **Besonders wichtig ist dies in Schulungssituationen**, in welchen der Tenant nach einigen Wochen automatisch gelöscht wird.

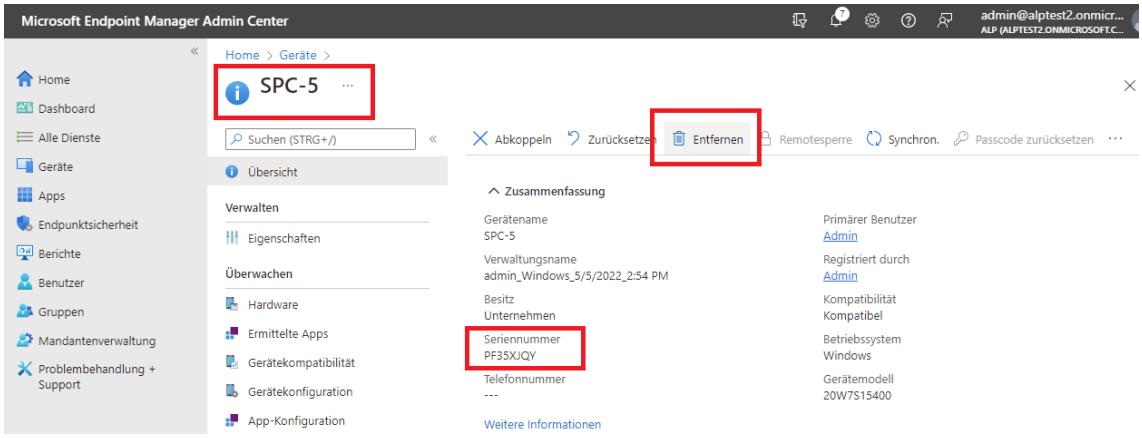
Der Versuch, das Autopilotgerät im Windows-Autopilot-Bereich (zu erreichen unter „Geräte – Geräte registrieren – Geräte“) direkt zu löschen, schlägt fehl:



Auf der Autopilot-Geräteseite kann man mit einem Klick auf das Gerät aber ablesen, unter welchem Namen es im Azure AD registriert ist:



Das Gerät muss nun im Bereich „Geräte – Windows“ aus dem Azure AD gelöscht werden:



Im letzten Schritt wird der Eintrag im Windows-Autopilot-Bereich (zu erreichen unter „Geräte – Geräte registrieren – Geräte“) entfernt. Dieser Vorgang dauert relativ lange, da der Eintrag aus Microsoft-Datenbanken gelöscht werden muss, die weltweit synchronisiert werden. Ein sofortiges Einbinden in einen anderen Tenant kann zu Problemen führen.

SOFTWARE MIT HERKÖMMLICHEM INSTALLATIONSPROGRAMM VERTEILEN

Um Software mit herkömmlichen Installationsprogrammen (setup.exe) zu verteilen, muss deutlich mehr Aufwand betrieben werden. Die hier beschriebene Methode setzt voraus, dass es einen „silent installer“ gibt, d.h. dass es möglich ist, das gewünschte Programm über die Kommandozeile zu installieren, ohne dass irgendwelche Meldungen bestätigt oder Fragen beantwortet werden müssen.
Beispiel: `setup.exe /quiet /norestart`
Eine Übersicht über die Befehle zur Installation gängiger Programme findet man auf Webseiten wie https://silentinstallhq.com/silent-install-knowledge-base.
Bevor die Software mit dem Endpoint Manager auf die Computer verteilt werden kann, muss aus dem Setup-Programm ein sogenanntes Intunewin-Paket erstellt werden. Dazu wird IntuneWinAppUtil.exe aus dem „Microsoft Win32 Content Prep Tool“ benötigt. Es wird kostenlos von Microsoft zum Download angeboten.
Zur Erzeugung der Intunewin-Pakete wird sinnvollerweise ein eigener Ordner auf der lokalen Festplatte des Administrations-PCs angelegt, hier der Ordner C:\AppPackaging. In diesen Ordner wird die Datei IntuneWinAppUtil.exe kopiert.
Für jede zu verteilende Software wird ein neuer Ordner erzeugt, in den alle zur Installation benötigten Dateien kopiert werden. Exemplarisch wird hier der Firefox-Browser paketiert, dessen Installationsprogramm „Firefox Setup xx.x.x.exe“ keine weiteren Dateien benötigt. Es wird in den Ordner C:\AppPackaging\Firefox\ kopiert. Um Problemen mit den Leerzeichen im Dateinamen vorzubeugen, wird die Setup-Datei umbenannt in ffsetup.exe.
Die Befehlszeile zur unbeaufsichtigten Installation von Firefox lautet

```
ffsetup.exe -ms
```

Zur eigentlichen Paketerstellung öffnet man eine Kommandozeile und wechselt in den Ordner C:\AppPackaging\Firefox. Die Syntax für das Paketierungstool lautet:

```
IntuneWinAppUtil.exe -c <SetupOrdner> -s <setup.exe ohne Parameter> -o
<AusgabeOrdner>
```

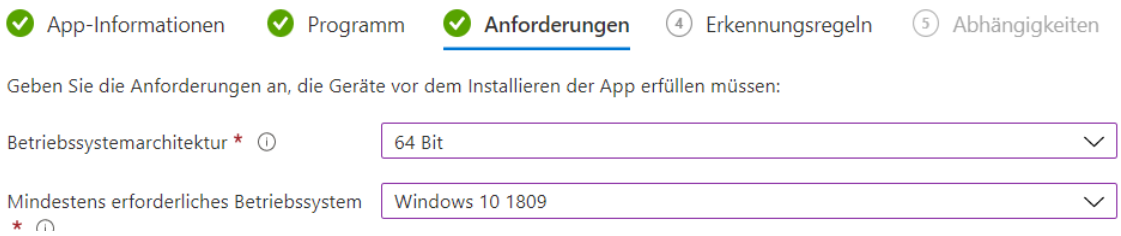
<SetupOrdner> ist der Ordner, der paketiert werden soll,
<AusgabeOrdner> ist der Ordner, in dem das fertige Intunewin-Paket abgelegt werden soll.
Die Parameter zur unbeaufsichtigten Installation werden erst später beim Hochladen im Endpoint Manager angegeben.
Für Firefox lautet die Befehlszeile also

```
..\IntuneWinAppUtil.exe -c . -s ffsetup.exe -o .
```

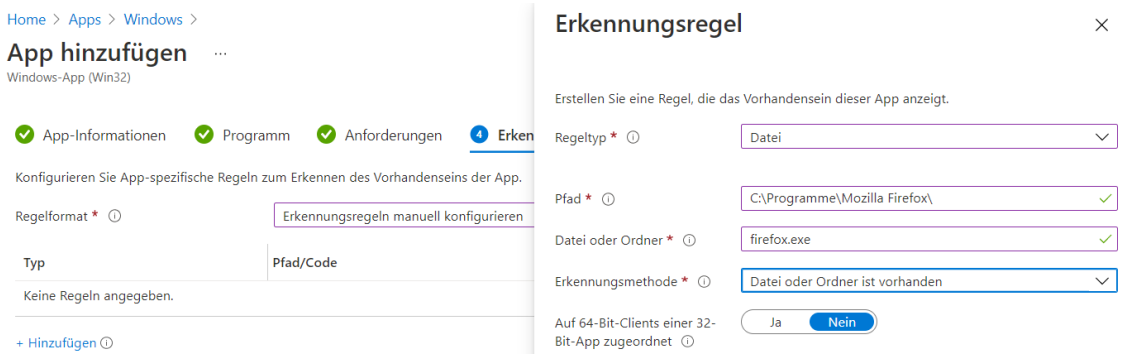
wobei „ . “ das aktuelle Verzeichnis kennzeichnet. Dort liegt nach Abschluss des Befehls das fertige Paket „ffsetup.intunewin“.
Dieses wird jetzt im Endpoint Manager mit folgenden Einstellungen hochgeladen:

- Apps -> Windows -> Hinzufügen -> App-Typ „Win32-App“
- App-Paketdatei auswählen: ffsetup.intunewin
- Beschreibung und Herausgeber beliebig, alle anderen Felder bleiben leer

- Auf Seite 2 wird der Installationsbefehl eingetragen:
  `ffsetup.exe -ms`
- Falls bekannt, kann der Deinstallationsbefehl eingegeben werden. Fehlt er, trägt man hier z.B.
  `echo`
  ein. Das Programm kann dann nicht über den Endpoint Manager deinstalliert werden, was normalerweise kein Problem darstellt.
- Die restlichen Einträge auf Seite 2 bleiben unverändert.
- Auf Seite 3 werden die erforderlichen Informationen eingetragen:



- Auf Seite 4 wird eine Erkennungsregel benötigt, anhand derer der Endpoint Manager die erfolgreiche Installation erkennen kann. Üblicherweise prüft man hier die Existenz des installierten Programms wie im Bild:



  Die genauen Pfade und Dateinamen ermittelt man auf einem PC, auf dem das entsprechende Programm zuvor manuell installiert wurde.
- Die Seiten „Abhängigkeiten“ und „Ablösung“ bleiben normalerweise leer.
- Auf der letzten Seite kann das Programm direkt Geräten oder Benutzern zugewiesen werden.

HINWEIS ZUM TESTEN DER SOFTWAREVERTEILUNG

Da die Endgeräte im ungünstigsten Fall erst nach 8 Stunden überprüfen, ob neue Software installiert werden soll, kann es lange dauern, bis die Software installiert wird. Im täglichen Schulbetrieb ist das normalerweise unproblematisch.
Um beim Testen der Softwareverteilung Wartezeiten zu vermeiden, kann man auf dem Endgerät in den Einstellungen auf der Seite „Auf Arbeits- oder Schulkonto zugreifen“ nach einem Klick auf „Info“ auf der folgenden Seite eine sofortige Synchronisierung auslösen. Alternativ kann der Computer neu gestartet werden. Dies löst ebenfalls eine Synchronisierung aus.

DRUCKER ÜBER POWERSHELL-SKRIPT EINBINDEN

Wird der Drucker nicht wie im letzten Abschnitt beschrieben erkannt, ist ein herkömmlicher Druckertreiber erforderlich. Der Treiber kann von der Herstellerhomepage bezogen oder mit einem Tool wie Double Driver von einer installierten Maschine kopiert werden.
Der Treiber wird über ein Powershell-Skript wie ein Softwarepaket verteilt.
Benötigt wird dazu folgendes Skript. Es wird z.B. nach C:\AppPackaging\Drucker\Testdrucker\InstallPrinter.ps1 gespeichert:

```
Start-Transcript -path "C:\Testdrucker.txt"

$PSScriptRoot = Split-Path -Parent -Path $MyInvocation.MyCommand.Definition
$DriverPath = "$PSScriptRoot\Driver"

# Die folgenden Zeilen anpassen:
$DriverName = "HP LaserJet MFP M232-M237 PCLm-S"
$DriverInf = "$PSScriptRoot\Driver\OEM29.inf"
$portName = "10.36.18.125"
$printerName = "Testdrucker"

$checkPortExists = Get-Printerport -Name $portname -ErrorAction
SilentlyContinue

if (-not $checkPortExists) {
  Add-PrinterPort -name $portName -PrinterHostAddress $portName
}
cscript "C:\Windows\System32\Printing_Admin_Scripts\de-DE\Prndrvr.vbs" -a -m
$DriverName -h $DriverPath -i $DriverInf
$printDriverExists = Get-PrinterDriver -name $DriverName -ErrorAction
SilentlyContinue

if ($printDriverExists)
{
  Add-Printer -Name $printerName -PortName $portName -DriverName $DriverName
}
else
{
  Write-Warning "Fehler bei der Druckertreiber-Installation"
}
```

Der Druckertreiber selbst (im cat/inf/sys-Format) wird in einen Unterordner „Driver“ kopiert. Der Ordner Testdrucker wird für jeden zu installierenden Drucker kopiert und passend zum Drucker benannt. Im Skript selbst müssen nur die erste Zeile (für die Ausgabe des Installationsprotokolls auf dem Endgerät) und die vier Zeilen nach dem Kommentar angepasst werden.

- Der $DriverName muss exakt zum Druckertreiber passen. Meist findet man den richtigen Namen in der .inf-Datei des Druckertreibers unter der Bezeichnung „MODEL“, im Bereich [OEM…] oder ganz am Ende der .inf-Datei im Abschnitt „Strings“.
- Bei $DriverInf ist der Name der INF-Datei einzutragen; Beispiel:
  $DriverInf = "$PSScriptRoot\Driver\OEM29.inf"
- $portName bezeichnet die IP-Adresse des Druckers, Beispiel:
  $portName = "10.2.200.201"
- $printerName ist die gewünschte Bezeichnung des Druckers; Leerzeichen im Namen sind möglich.

Soll statt des normalerweise verwendeten RAW-Protokolls der Drucker über das LPR-Protokoll angesprochen werden (vor allem bei Kopiersystemen üblich), ändert sich die Zeile zum Hinzufügen des PrinterPorts zu

```
Add-PrinterPort -name $portName -LprHostAddress $portName -LprQueueName "lp"
```

Es sind auch zusätzliche Anpassungen möglich, z.B. standardmäßiger einseitiger oder Schwarz-weiß-Druck. Hierzu wird unter der Zeile "Add-Printer ..." ergänzt:

```
Set-PrintConfiguration -PrinterName $printerName -DuplexingMode
OneSided -Color $false
```

Damit der Drucker bei Bedarf auch wieder deinstalliert werden kann, legt man ein zweites Skript namens RemovePrinter.ps1 mit folgendem Inhalt an:

```
Remove-Printer -name "Testdrucker"
Remove-Item "C:\Testdrucker.txt"
```

Um die Funktionsfähigkeit ohne die Verteilung über den Endpoint Manager zu prüfen, sollte der gesamte Ordner manuell auf ein Endgerät kopiert und das Skript dort händisch mit dem unten genannten Installationsbefehl getestet werden.
Für die Verteilung über den Endpoint Manager muss der Treiber mit dem Skript wie ein Softwarepaket in ein Intunewin-Paket konvertiert werden:

```
cd C:\AppPackaging\Drucker\Testdrucker
..\..\IntuneWinAppUtil.exe -c . -s Testdrucker.ps1 -o .
```

Besondere Einstellungen bei der Verteilung:

- Installationsbefehl:
  `powershell.exe -executionpolicy bypass -file .\Testdrucker.ps1`
- Deinstallationsbefehl = echo
- Erkennungsregel = Datei aus Zeile 1 im Skript (Testdrucker.txt) vorhanden:

EINSTELLUNGEN AN ENDGERÄTEN

Über den Endpoint Manager kann man nahezu jede Windows-Einstellung auf den Endgeräten verändern, ähnlich wie es bei Verwendung eines Domänencontrollers mit Gruppenrichtlinien möglich ist. Die allermeisten Einstellungen haben bereits sinnvolle Standardwerte. Hier wird exemplarisch eine Einstellung vorgestellt, die angepasst werden soll.

BILDSCHIRMSPERRE BEI GEMEINSAM GENUTZTEN GERÄTEN

Wird ein PC abwechselnd von verschiedenen Benutzern verwendet (z.B. PCs in Klassenzimmern oder Computerräumen), vergessen die Benutzer manchmal, sich abzumelden. Daher ist es sinnvoll, das Gerät nach einer gewissen Zeit ohne Eingaben automatisch zu sperren. Die zugehörige Einstellung ist leider nicht direkt über die Konfigurationsoberfläche des Endpoint Manager erreichbar, sondern muss als sogenannte OMA-URI („Open Mobile Alliance – Uniform Resource“) eingebunden werden.
Dazu erzeugt man im Bereich Geräte / Konfigurationsprofile ein neues Profil für Windows 10 und höher und wählt dort unter Vorlagen „Benutzerdefinierte Vorlage hinzufügen“. Als OMA-URI wird
`./Vendor/MSFT/Policy/Config/LocalPoliciesSecurityOptions/InteractiveLogon_MachineInactivityLimit`
(ohne Zeilenumbruch) eingetragen, als Datentyp „Ganze Zahl“ gewählt und als Wert das gewünschte Bildschirmsperre-Timeout in Sekunden angegeben.
Abschließend wird das neue Profil den gewünschten Geräten zugewiesen.

ARBEITEN MIT SKRIPTEN

BEREITSTELLEN VON DATEIEN AUF DEM DESKTOP

Sollen auf dem Desktop der Endgeräte Verknüpfungen oder Skripte abgelegt werden, lässt sich dies ebenfalls über die Softwareverteilung des Endpoint Managers erreichen.
Beispielskript:

```
Start-Transcript "C:\scripts\KopiereAufDesktopSharedPC.txt"
$Ziel = "C:\Users\Public\Desktop"

If(!(test-path "C:\scripts"))
{
  New-Item -Path "C:\" -Name "scripts" -ItemType "Directory"
}

Copy-Item -Path ".\PublicDesktop\*.*" -Destination $Ziel -Recurse
```

Dieses Skript wird zusammen mit einem Ordner PublicDesktop, der die gewünschten Desktop-Verknüpfungen oder Skripte enthält, auf dem üblichen Weg paketiert und verteilt. Auf dem Endgerät kopiert es alle Dateien aus dem Ordner PublicDesktop in den Ordner, in dem Windows die Dateien speichert, die bei allen Benutzern auf dem Desktop angezeigt werden sollen.

AUTOMATISCHES HERUNTERFAHREN AM TAGESENDE

Das folgende Skript erstellt auf dem Endgerät eine geplante Aufgabe, die auf dem Endgerät täglich um 17 Uhr das Skript „Shutdown5min.cmd“ ausführt.

CreateShutdownDailyTask.ps1:

```
If(!(test-path "C:\scripts"))
{
  New-Item -Path "C:\" -Name "scripts" -ItemType "Directory"
}
Copy-Item -Path ".\Shutdown5min.cmd" -Destination
"C:\scripts\Shutdown5min.cmd" -Force
$Action = New-ScheduledTaskAction -Execute "C:\scripts\Shutdown5min.cmd"
$Trigger = New-ScheduledTaskTrigger -Daily -At "17:00"
$Trigger.StartBoundary =
[DateTime]::Parse($Trigger.StartBoundary).ToLocalTime().ToString("s")
$Principal = New-ScheduledTaskPrincipal -UserId "NT AUTHORITY\SYSTEM" -
LogonType ServiceAccount -RunLevel Highest
Register-ScheduledTask -TaskName "Shutdown1700" -Action $Action -Trigger
$Trigger -Principal $Principal

// Die Zeile mit StartBoundary bewirkt, dass die Zeit nicht in UTC, sondern in
lokaler Zeit übergeben wird.
// Ansonsten wird bei der Zeitumstellung der Shutdown-Zeitpunkt um eine Stunde
verschoben!
```

Shutdown5min.cmd:

```
shutdown /s /f /t 300
```

Beide Skripte werden in einen gemeinsamen Ordner gespeichert, auf dem üblichen Weg zu CreateShutdownDailyTask.intunewin paketiert und mit dem Endpoint Manager als Win32-App verteilt.

ANLEGEN EINES LOKALEN ADMIN-BENUTZERS

Zur Fehlersuche ist es hilfreich, auf den Endgeräten einen lokalen Admin-Benutzer anzulegen. Dies kann über folgendes Skript „CreateLocalAdmin.ps1“ gemacht werden:

```
$Username = "admin2"
$Password = "12345"

$group = "Administratoren"

$adsi = [ADSI]"WinNT://$env:COMPUTERNAME"
$existing = $adsi.Children | where {$_.SchemaClassName -eq 'user' -and $_.Name
-eq $Username }

if ($existing -eq $null) {

Write-Host "Creating new local user $Username."
& NET USER $Username $Password /add /y /expires:never

Write-Host "Adding local user $Username to $group."
& NET LOCALGROUP $group $Username /add

}
else {
Write-Host "Setting password for existing local user $Username."
$existing.SetPassword($Password)
}

Write-Host "Ensuring password for $Username never expires."
& WMIC USERACCOUNT WHERE "Name='$Username'" SET PasswordExpires=FALSE
```

Dieses Skript wird über den Endpoint Manager -> Geräte -> Skripts allen Geräten zugewiesen. Eine Paketierung ist nicht notwendig.

WEITERFÜHRENDE INFORMATIONEN

Auf den Internetseiten von SCHULNETZ (schulnetz.alp.dillingen.de) finden Sie begleitend zum Laborbuch unter dem Gliederungspunkt „Materialien“ weiterführende Informationen zu den Kursinhalten, sowie eine PDF-Fassung des Laborbuches zum Download:

Zudem werden regionale sowie Lehrgänge an der Akademie Dillingen aufgeführt.