

HANDBUCH – UNIFIED ENDPOINT MANAGEMENT (VMWARE WORKSPACE ONE)

Version 2.9.2, letzte Änderung: 03.07.2024

Änderung in Handbuch-Version 2.9.2:

- Kapitel 10 [iPadOS Profil erstellen](#) überarbeitet

Ältere Änderungen sind in der [Änderungshistorie](#) aufgeführt.

1	Einleitung.....	3
2	Login	4
3	Wo finde ich was?	5
3.1	Titelleiste.....	5
3.2	Monitor	5
3.3	Geräte.....	6
3.4	Konten	8
3.5	Apps & Bücher	9
3.6	Gruppen & Einstellungen	10
4	Einbinden eines Testgerätes	12
4.1	Windows: Einbinden von Testgeräten	12
4.2	iPadOS: Einbinden von Testgeräten	19
4.3	Windows und iPadOS: Testgeräte im UEM verschieben	29
4.4	Windows und iPadOS: Testgerät aus dem UEM entfernen	31
4.5	Basic-Benutzer: Passwort zurücksetzen.....	32
5	Anlegen von Benutzergruppen	33
6	Anlegen von Zuweisungsgruppen (Smartgroups)	35
7	Anlegen von Nutzungsbedingungen	37
8	iPadOS: Anbindung des Apple School Managers für die App-Verteilung	39
9	iPadOS: App-Kauf, -Installation, -Deinstallation	42
9.1	App-Einkauf	42
9.2	App-Installation	43
9.3	App-Deinstallation	46

9.4	App-Konfiguration verteilen	50
10	iPadOS: Profil erstellen.....	52
11	iPadOS: Schriftarten hinzufügen.....	55
12	iPadOS: Kennung zurücksetzen	57
13	iPads: Gerät zurücksetzen.....	58
14	Windows: Paket-Erstellung, -Installation und -Deinstallation.....	59
14.1	Paket-Erstellung	59
14.2	Paket-Aktualisierung.....	64
14.3	Paket-Installation	65
14.4	Paket-Deinstallation.....	67
14.5	Lizenzverteilung.....	69
14.6	Paketierung Microsoft Office.....	72
14.7	Paketierung Microsoft-Store-App.....	74
15	Windows: Kopieren von Dateien/Ordnern.....	77
16	Windows: Profil erstellen	83
17	Windows: Passwort oder Endgerät zurücksetzen	86
17.1	Windows Passwort zurücksetzen.....	87
17.2	Windows: Gerät zurücksetzen	89
17.3	DataportResetTool.....	90
18	Windows: Netzlaufwerk verteilen	91
18.1	Variante 1: Verteilung eine CFG-Datei.....	91
18.2	Variante 2: Verteilung einer JSON-Datei.....	93
19	Windows: Skripte verteilen.....	96
19.1	Nutzungsszenarien von Skripten	96
19.2	Vorbereitung.....	96
19.3	Skript (Datei) anlegen	96
19.4	Produkt anlegen und aktivieren.....	99
20	Änderungshistorie.....	103

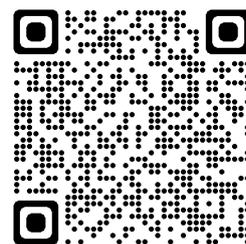
1 Einleitung

Die Lehrkräfte-Endgeräte des Landes Schleswig-Holstein sind in einem Unified Endpoint Management (UEM) – einer zentralen Verwaltung für Endgeräte – eingebunden. Die Endgeräte werden bei der Erstbenutzung durch Lehrkräfte am UEM angemeldet und erhalten dabei bestimmte durch das Land bereitgestellte Richtlinien sowie eine Grundausrüstung an Software. Zusätzliche Software kann durch Lehrkräfte über den internen Appstore (Hub) nachinstalliert werden. Auf den Lehrkräfte-Endgeräten (Windows) lassen sich zudem auch ohne den internen Appstore Anwendungen installieren. Software darf durch die jeweilige Lehrkraft jedoch nur installiert werden, wenn diese Software durch die Schulleitung geprüft und freigegeben wurde.

Neben der grundlegenden Konfiguration der Endgeräte und der Bereitstellung der Software-Grundausrüstung ist die zentrale Administration des Landes auch für den technischen Support, den Gerätetausch (Vor-Ort-Service) sowie die Passwort- und Gerätezurücksetzung zuständig.

Nähere Informationen zum UEM und den Lehrkräfte-Endgeräten (u. a. die bereitgestellte Software) erhalten Sie auf der folgenden Infoseite:

<https://medienberatung.igsh.de/endgeraete-lk-schultraeger.html>.



Falls gewünscht können Schulträger, BBS und RBZ die dezentrale Administration der Lehrkräfte-Endgeräte über das Unified Endpoint Management (UEM) „Workspace One“ übernehmen. Diese umfasst vor allem die Bereitstellung schul- bzw. schulträgerindividueller Software und Einstellungen. Zusätzliche Software darf auch hier nur nach Prüfung und Freigabe durch die jeweilige Schulleitung bereitgestellt werden.

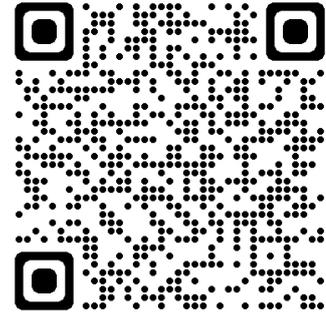
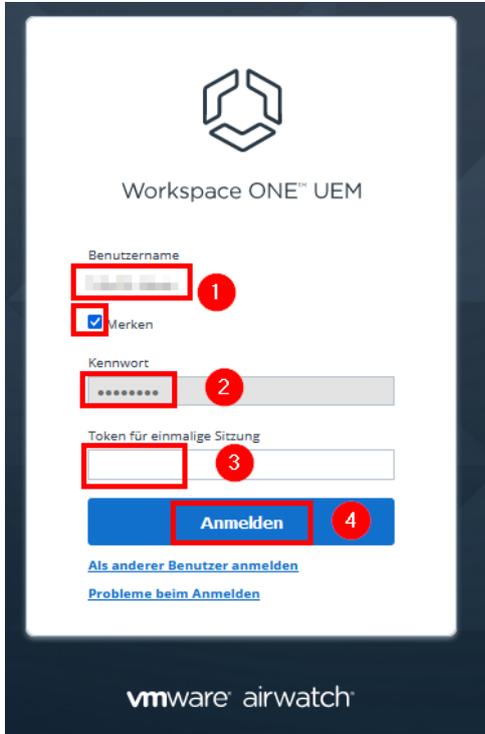
Das Land hat auf den Geräten Sicherheitsrichtlinien aktiviert und kümmert sich mit Hilfe der in Windows 10 integrierten Anwendungen um die Gerätesicherheit, den Viren- und Bedrohungsschutz sowie um Firewall-Einstellungen. Eine Installation zusätzlicher Sicherheitssoftware ist daher nicht erforderlich und kann ggf. dazu führen, dass vorhandene Sicherheitseinstellungen außer Kraft gesetzt werden.

Zur Administration zugelassene Personen sind Mitarbeiter und Mitarbeiterinnen des Schulträgers, IT-Dienstleister, die mit der Verwaltung der Lehrkräfteendgeräte beauftragt wurden, sowie IT-Personal von berufsbildenden Schulen/RBZ. Explizit sind keine Lehrkräfte allgemeinbildender Schulen zugelassen.

Diese Anleitung gibt einen Überblick über die wichtigsten Funktionen und Bedienelemente des UEM.

2 Login

Nach Aufruf der Webadresse <https://uem-console.dataport.de> gelangt man zunächst auf die Loginseite des UEM:



Nach Eingabe des Benutzernamens (1) und des Passworts (2) auf der Startseite des UEM wird ein Token an Ihre im UEM registrierte E-Mail-Adresse gesendet. Nach Eingabe dieses Tokens (3) und Bestätigung mit „Anmelden“ (4) gelangt man auf das Dashboard des UEM.

Hinweis: Der Benutzername besteht im Normalfall aus den ersten fünf Buchstaben des Nachnamens, den ersten beiden Buchstaben des Vornamens und der Endung „-Admin“.

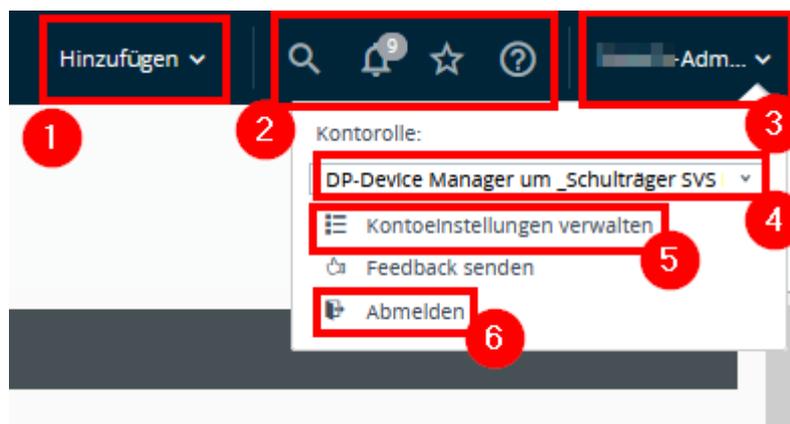
3 Wo finde ich was?

3.1 Titelleiste

Auf der linken Seite der Titelleiste findet man die Einstellmöglichkeiten zu den zugehörigen Organisationseinheiten. Hier kann man – die passenden Rechte vorausgesetzt – auf die Ebene des Schulträgers bzw. auf die Ebenen einzelner Schulen wechseln. Man bekommt dann jeweils nur die Informationen (z. B. Geräte, Benutzer, Profile) dieser gewählten Einheit angezeigt:



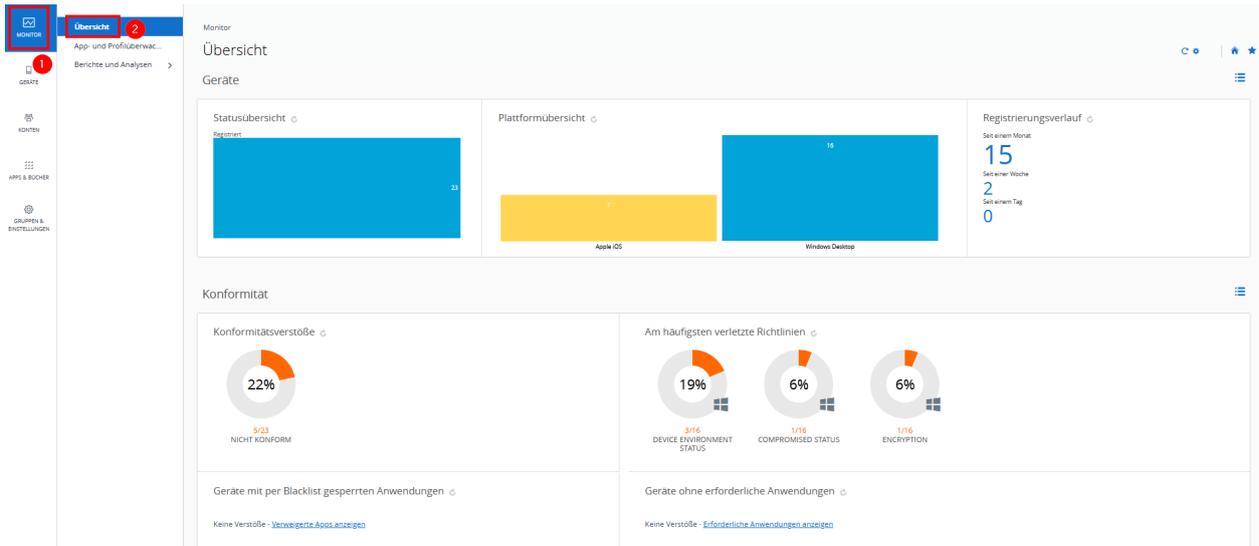
Auf der rechten Seite der Titelleiste findet man weitere Funktionen und Einstellmöglichkeiten:



- 1: Schnellauswahl zum Hinzufügen z. B. von Benutzern oder Profilen
- 2: Suche, Benachrichtigungen, Lesezeichen und Hilfe
- 3: Menü der Kontoeinstellungen. Hier kann zum Beispiel das Passwort des eigenen UEM-Admin-Accounts geändert werden.
- 4: Umstellmöglichkeit der Administrator-Rolle (z. B. Device-Manager auf Schulträger oder Schulebene bzw. Device-Manager eines anderen Schulträgers)
- 5: Kontoeinstellungen wie z. B. Benutzerdaten, Benachrichtigungen und Kennwort
- 6: Logout

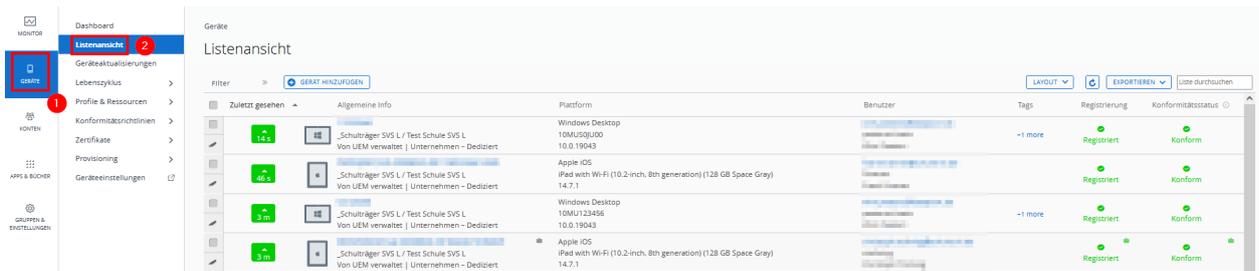
3.2 Monitor

Über den Menüpunkt „Monitor“ (1) erhält man einen groben Überblick über alle in der jeweiligen Ebene (Schulträger, Schule) befindlichen Geräte (2):

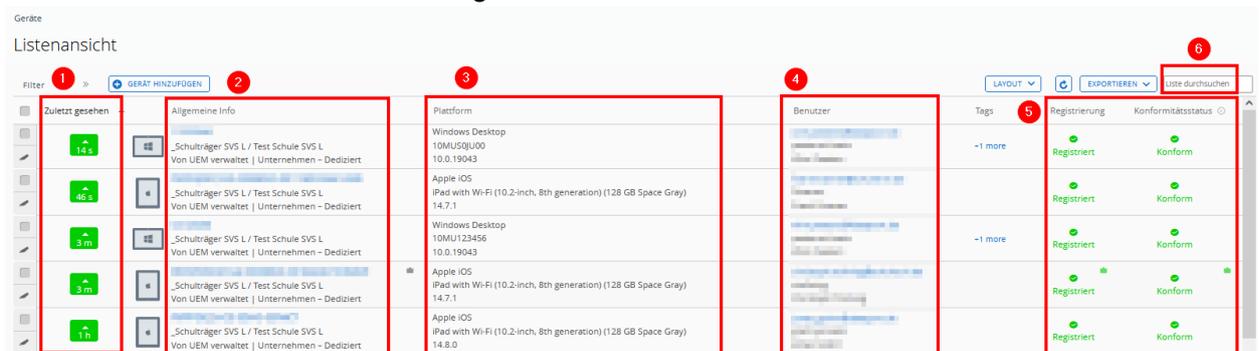


3.3 Geräte

Unter dem Menüpunkt „Geräte“ (1) befinden sich alle gerätespezifischen Einstellmöglichkeiten, zum Beispiel die Listenansicht aller Geräte (2):



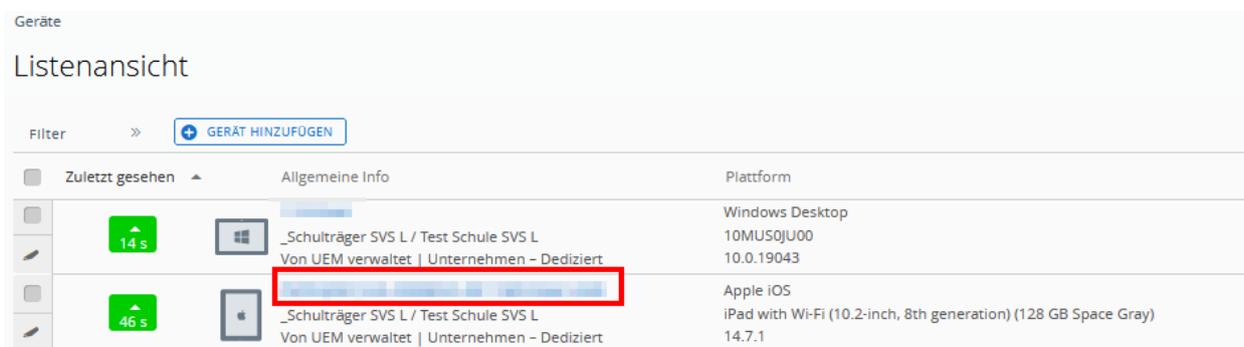
Man erhält in der Listenübersicht folgende Informationen:



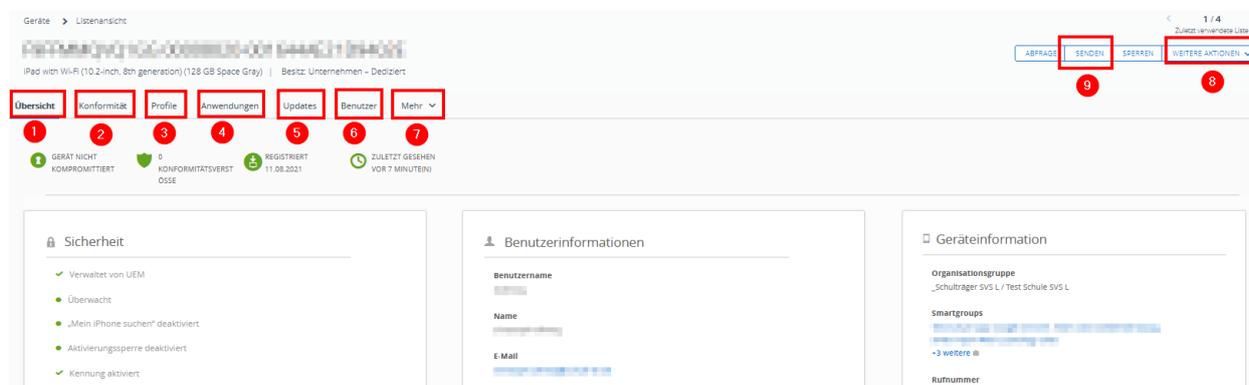
- 1: Vergangene Zeit seit der letzten Verbindung des Gerätes mit dem UEM
- 2: Seriennummer, Zugehörigkeit zur Organisationsgruppe (Schulträger/Schule)
- 3: Betriebssystem, Version des Betriebssystems
- 4: Benutzer des Gerätes (registrierte Mailadresse, Benutzername und vollständiger Name)
- 5: Status zur Registrierung am UEM und zur Konformität

Über die Eingabe eines Begriffes (Benutzername, Betriebssystem, Seriennummer) im Suchfeld (6) lässt sich die Anzeige auf bestimmte Geräte reduzieren.

Detaillierte Informationen zu einem Gerät erhält man per Klick auf die Seriennummer des betreffenden Gerätes in der Listenansicht:



Es erscheint dann die Detailansicht des Gerätes:



Über die verschiedenen Reiter erhält Informationen zu folgenden Bereichen:

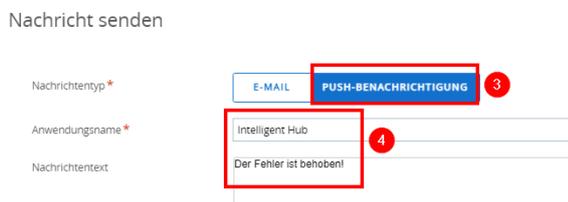
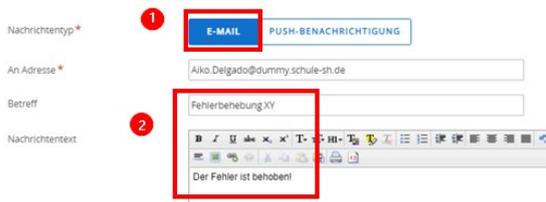
- 1: Schnellüberblick über alle Gerätedetails
- 2: Detailinformationen zum Konformitätsstatus
- 3: Liste der Richtlinien, die regelmäßig auf Konformität geprüft werden
- 4: Liste der installierten Anwendungen (installiert oder nicht installiert, verwaltet oder selbst installiert, Versionsnummer)
- 5: Liste der installierten Betriebssystem-Updates (Art des Updates)
- 6: Benutzerdetails
- 7: Weitere Details zu verschiedenen Bereichen (z. B. Netzwerk und Sicherheit). Hier ist insbesondere der Bereich „Fehlerbehebung“ wichtig, in dem Statusinfos zu aufgetretenen Problemen aufgelistet werden.

Über den Menüpunkt „Weitere Aktionen“ (8) kann man u.a. folgende Aktionen durchführen:

- Informationen zu bestimmten Gerätedetails (Sicherheit, Anwendungen usw.) anfordern
- Gerät neu starten
- Gerät zurücksetzen
- bei iPads: Geräte-Kennung zurücksetzen

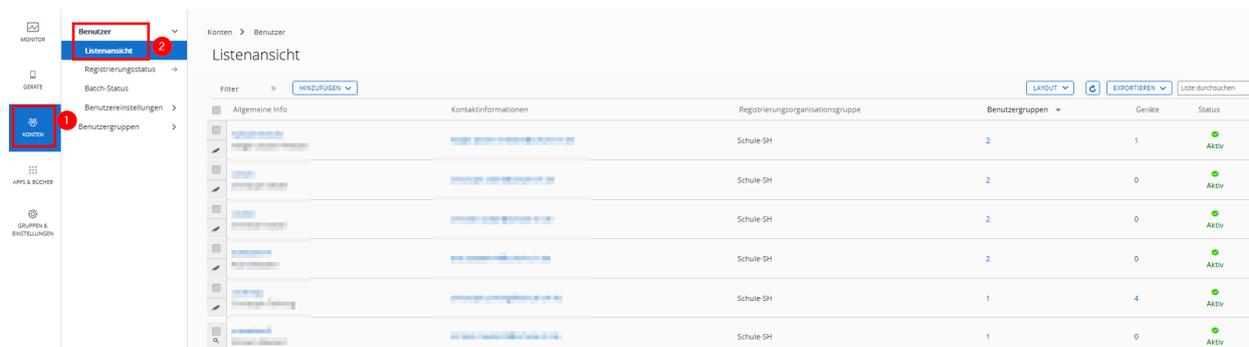
Über „Senden“ (9) lassen sich Nachrichten (2+4) zum Beispiel zur Fehlerbehebung direkt an den Benutzer per E-Mail (1) oder alternativ als Push-Nachricht in den internen Appstore (Hub) auf dem jeweiligen Endgerät versenden:

Nachricht senden

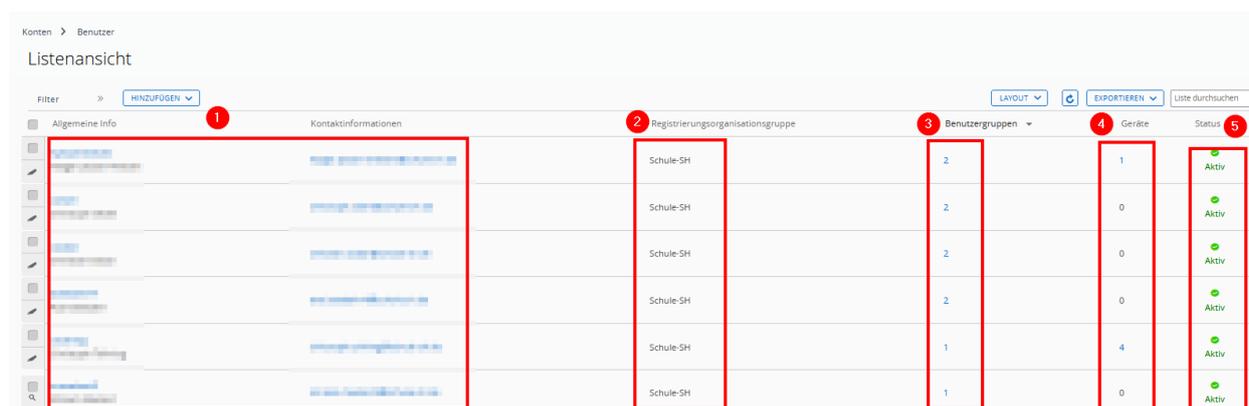


3.4 Konten

Unter dem Menüpunkt „Konten“ (1) befinden sich alle benutzerspezifischen Einstellmöglichkeiten, zum Beispiel die Listenansicht aller Benutzer (2) einer Schule bzw. eines Schulträgers:

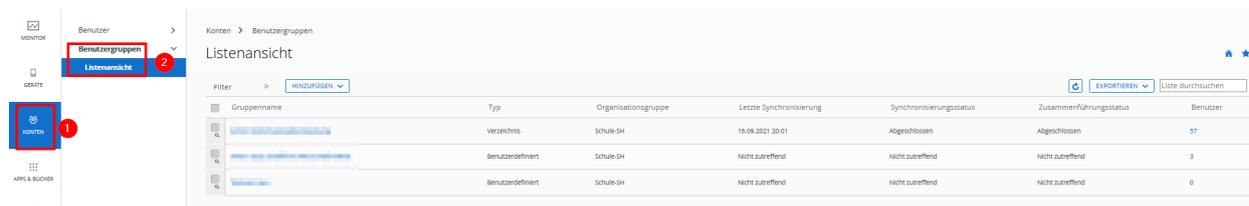


Man erhält in der Listenübersicht folgende Informationen:

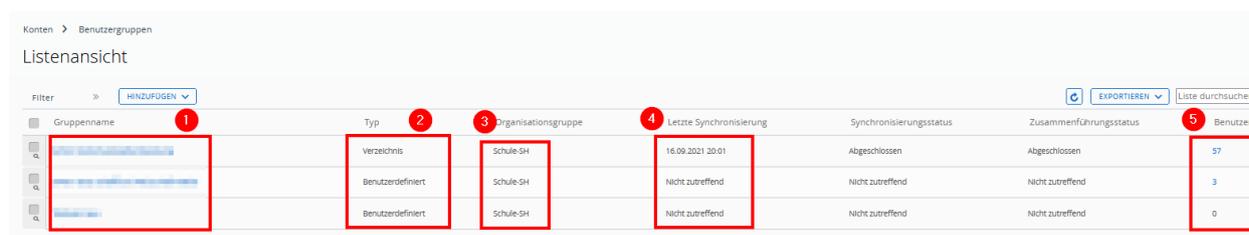


- 1: Benutzerdetails: Anmeldenname, Benutzername, E-Mail-Adresse
- 2: Organisationsgruppe (Land, Schulträger, Schule), die den Benutzer bzw. die Benutzerin angelegt hat
- 3: Anzahl der Benutzergruppen, in denen der Benutzer bzw. die Benutzerin Mitglied ist
- 4: Anzahl der auf den Benutzer bzw. die Benutzerin registrierten Endgeräte
- 5: Status des Benutzers bzw. der Benutzerin

Über die Auswahl „Konten“ (1) und „Benutzergruppen“ – „Listenansicht“ (2) erhält man Informationen zu vorhandenen Benutzergruppen:



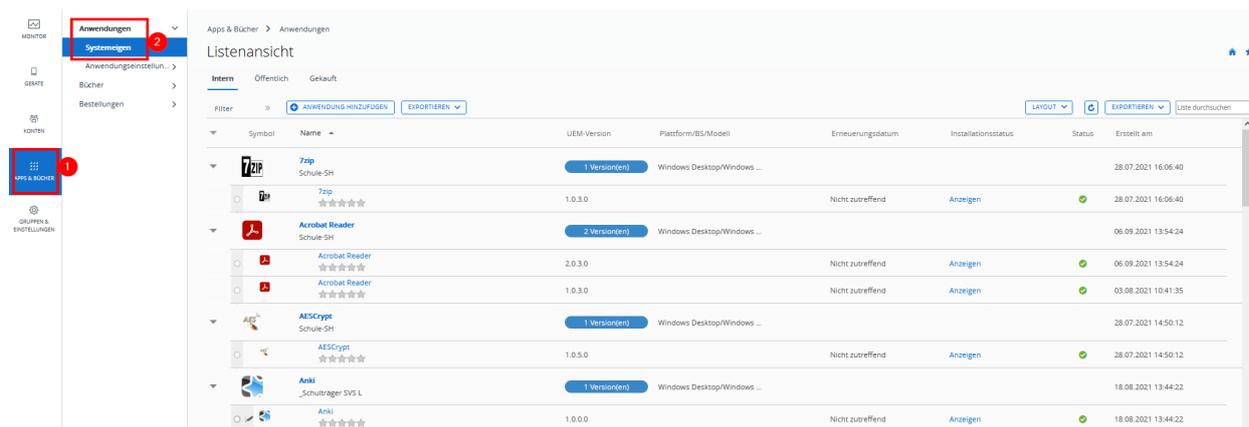
Man erhält in der Listenübersicht folgende Informationen:



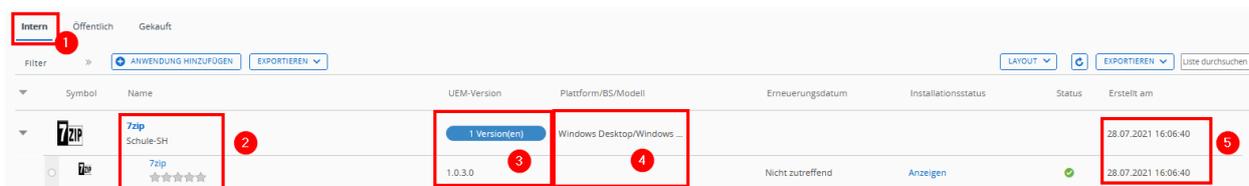
- 1: Gruppenname
- 2: Gruppentyp (Verzeichnisgruppe oder benutzerdefinierte Gruppe)
- 3: Organisationsgruppe (Land, Schulträger, Schule), die die Gruppe erstellt hat
- 4: Datum und Uhrzeit der letzten Synchronisierung (nur bei den vorangelegten Lehrer-Gruppen einer Schule)
- 5: Anzahl der Gruppenmitglieder

3.5 Apps & Bücher

Unter dem Menüpunkt „Apps & Bücher“ (1) befinden sich alle Einstellmöglichkeiten zu Anwendungen, zum Beispiel die Listenansicht über vorhandene Software (2):

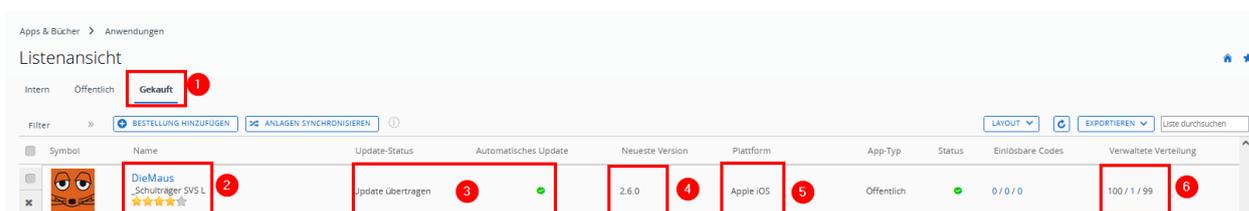


Unter dem Reiter „Intern“ (1) befinden sich die erstellten Softwarepakete für die Windows-Endgeräte:



- 2: Software-/Paketname
- 3: Softwareversion
- 4: Betriebssystem
- 5: Erstellungsdatum

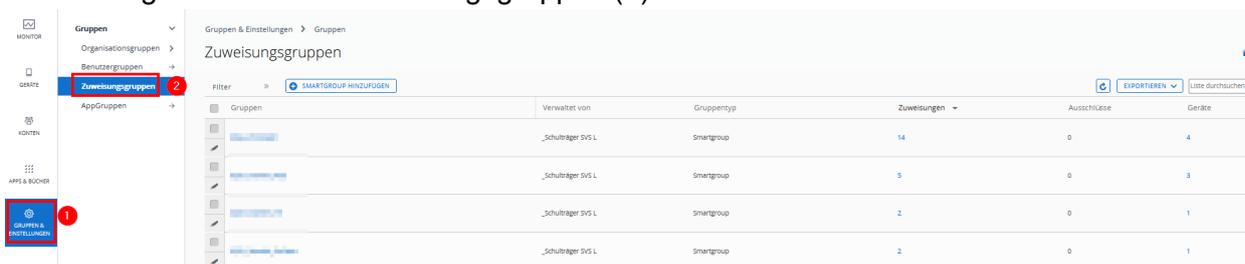
Unter dem Reiter „Gekauft“ (1) befinden sich die über den Apple School Manager bezogenen Apps für die iPads:



- 2: Name der App und der verwaltenden Organisationsgruppe (Land, Schulträger, Schule)
- 3: Information über den Update-Status und die Update-Aktivierung
- 4: App-Versionsnummer
- 5: Betriebssystem
- 6: Anzahl der insgesamt vorhandenen/zugewiesenen/noch nicht zugewiesenen Lizenzen

3.6 Gruppen & Einstellungen

Unter dem Menüpunkt „Gruppen & Einstellungen“ (1) befinden sich zum Beispiel die Einstellmöglichkeiten der Zuweisungsgruppen (2):



Eine Zuweisungsgruppe besteht aus einer Benutzergruppe bzw. einzelnen Benutzern bzw. Geräten und zusätzlichen Einstellmöglichkeiten (z.B. Betriebssystem, Ausschlüsse). Sie dient zum Beispiel der passgenauen Zuweisung von Software und Profilen.

Man erhält in der Listenübersicht folgende Informationen:

Gruppen & Einstellungen > Gruppen

Zuweisungsgruppen

Filter > SMARTGROUP HINZUFÜGEN

EXPORTIEREN Liste durchsuchen

Gruppen	Verwaltet von	Gruppentyp	Zuweisungen	Ausschlüsse	Geräte
[Redacted] 1	_Schulträger SVS L 2	smartgroup	14 3	0 4	4 5
[Redacted]	_Schulträger SVS L	smartgroup	5	0	3
[Redacted]	_Schulträger SVS L	smartgroup	2	0	1
[Redacted]	_Schulträger SVS L	smartgroup	2	0	1

- 1: Gruppenname
- 2: Organisationsgruppe (Land, Schulträger, Schule), die die Gruppe verwaltet
- 3: Anzahl der zugehörigen Zuweisungen (z.B. Apps und Profile)
- 4: Anzahl der Ausschlüsse, also Nichtzuweisung bestimmter Apps und Profile
- 5: Anzahl der zugehörigen Geräte

4 Einbinden eines Testgerätes

Bei Bedarf können Administratorinnen und Administratoren schulträgereigene Endgeräte ins UEM einbinden, um zum Beispiel Profil- und App-Installationen vor dem Rollout hier testen zu können.

Wichtige Hinweise:

- Es dürfen dabei **maximal zwei Geräte pro allgemeinbildende Schule bzw. vier Geräte pro berufsbildende Schule** eingebunden werden.
- Diese müssen bei der Einrichtung und Anmeldung im UEM einem pro Admin-Account angelegten **Basic-Benutzer-Account** bestehend aus den ersten fünf Buchstaben des Nachnamens, den ersten beiden Buchstaben des Vornamens und der Endung „-basic“ (z. B. „MusteMa-basic“) zugewiesen werden.
- **Bei einem Schulträger mit mehreren Schulen:** Wenn zum Zeitpunkt der UEM-Account-Beantragung noch nicht die Auftragsvertragsverträge (AVV) aller Schulen vorliegen, hat der Admin-Account noch keinen Zugriff auf die Schulträgerebene. In diesem Fall wird auch der Basic-Benutzer-Account nicht auf der Schulträgerebene, sondern auf der Ebene einer Schule angelegt. Testgeräte würden in diesem Fall dann dieser Schule zugeordnet werden.
- Bei der Geräte-Anmeldung im UEM wird das Speichermedium des Gerätes verschlüsselt, die Sicherheitsrichtlinien angewendet sowie eine Grundausstattung an Software installiert. Um ein Testgerät bei Bedarf wieder aus dem UEM abzumelden ist eine komplette **Zurücksetzung des Gerätes** erforderlich.

4.1 Windows: Einbinden von Testgeräten

Das einzubindende Endgerät (Windows) muss folgende Voraussetzungen erfüllen:

- TPM-Chip 2.0
- UEFI mit Secure Boot
- aktuelle Version von Windows 10 Professional/Education/Enterprise (Version 21H1)
- Empfehlung: Windows 10 neu installieren bzw. komplett zurücksetzen
- Gerät darf nicht in einer anderen Verwaltung bzw. in einer Domäne Mitglied sein

4.1.1 Windows: Testgerät im UEM registrieren

Hinweis: Im UEM können nur Geräte aufgenommen werden, die vorher im UEM bekannt gemacht worden sind. Für die Registrierung wird die Seriennummer des Endgerätes benötigt.

Zum Herausfinden der Seriennummer die Windows-Eingabeaufforderung aufrufen und nachfolgenden Befehl eingeben:

wmic bios get serialnumber

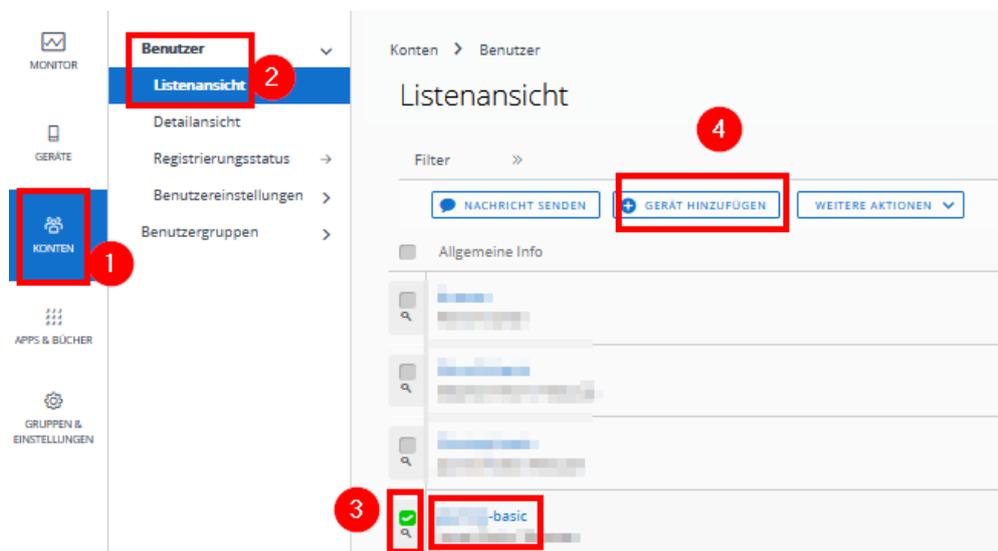
 Eingabeaufforderung

```
C:\Users>wmic bios get serialnumber
SerialNumber
02852
```

Die Seriennummer (Wichtig: inklusive führender Nullen) in den Zwischenspeicher kopieren.
 Wechseln Sie ins UEM und wählen zunächst oben am Bildschirmrand die Schulträger-Ebene aus:



Im Anschluss unter dem Menüpunkt „Konten“ (1) – „Benutzer“ – „Listenansicht“ (2) den vorangelegten Basic-Benutzer (mit der Endung „-basic“) auswählen (3) und auf „Gerät hinzufügen“ (4) klicken:



Hinweis: Der Name des Benutzers besteht aus den ersten fünf Buchstaben des Nachnamens, den ersten beiden Buchstaben des Vornamens und der Endung „-basic“ (Beispiel: MusteMa-basic).

In den Gerätedetails Plattform auf „Windows Desktop“ (1) umstellen, den Haken für erweiterte Optionen (2) setzen, die oben ermittelte Seriennummer des Gerätes eingeben (3), im Feld Anlagennummer "Testgerät" eingeben und den Nachrichtentyp auf „Keine(r/s)“ umstellen:

Gerät hinzufügen

General

Anzeigename: -basic Gerät

Organisationsgruppe: Test Schule SV5 L

Gerätebesitztyp: Unternehmen - Dediziert

Plattform: Windows Desktop **1**

Erweiterte Optionen zu Gerätedaten anzeigen **2**

Modell: Beliebige

BS: Beliebige

UDID:

Seriennummer: 0285...3 **3**

IMEI:

SIM:

Anlagennummer: Testgerät **4**

Message

Nachrichtentyp: **5** KEINE(R/S) E-MAIL SMS

Die Eingaben mit „Speichern“ bestätigen und damit die Registrierung abschließen.

Das registrierte Gerät sollte nun unter „Geräte“ (1) – „Lebenszyklus“ – „Registrierungsstatus“ (2) auftauchen (3):



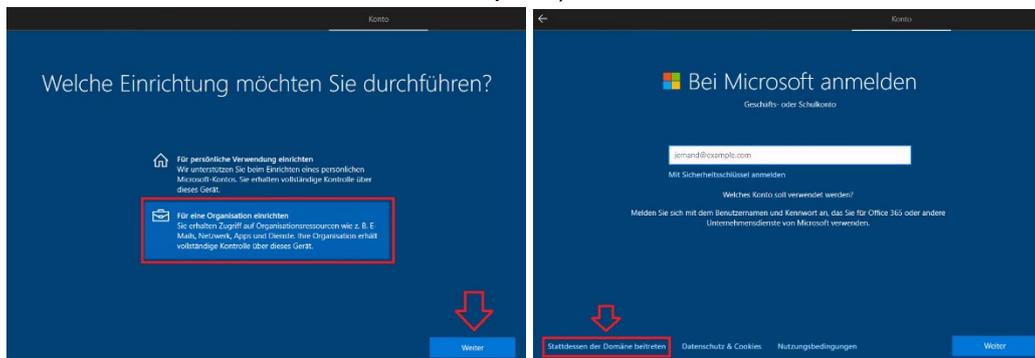
Hinweis: In dieser Liste können ausgewählte Geräte auch wieder gelöscht werden, wenn sie zum Beispiel nicht genutzt werden bzw. wenn bei der Registrierung Angabe falsch eingetippt wurden.

4.1.2 Windows: Testgerät vorbereiten

Hinweis: Auf dem Gerät muss eine aktuelle Version von Windows 10 Professional, Education bzw. Enterprise verwendet werden. Wir empfehlen eine Neuinstallation. Wenn nicht anders möglich, kann auch ein bereits eingerichtetes Gerät (mit lokalem Benutzerkonto, ohne Domänenanbindung und Fremdverwaltung) im UEM eingebunden werden. Fahren Sie in diesem Fall mit der Installation des Intelligent Hubs (siehe unten) fort.

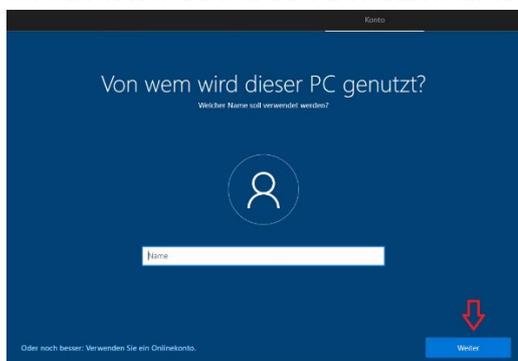
Bei einer Erst-Einrichtung zunächst ein lokales Konto ohne Kennwort einrichten. Dazu müssen bei der Windows-Einrichtung folgende Schritte vorgenommen werden:

- „Für eine Organisation einrichten“ (gilt nur für Windows Professional) wählen und im nächsten Schritt die Schaltfläche "Stattdessen der Domäne beitreten" (gilt für Windows 10 Professional, Education und Enterprise) wählen:



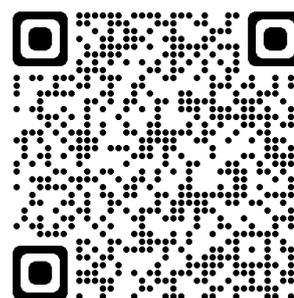
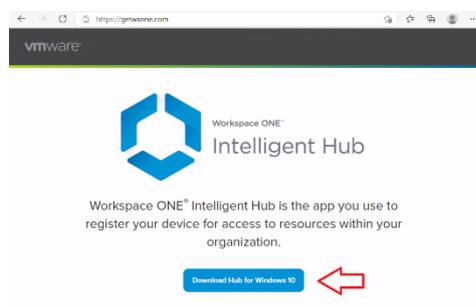
Hinweis: Das Gerät wird in keiner Domäne registriert, sondern lediglich ein lokales Konto angelegt.

- Im nächsten Schritt den Benutzernamen eingeben und **ohne** Kennwort fortfahren:

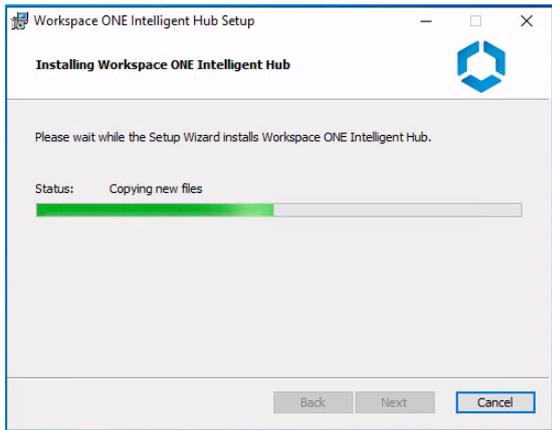


- Im Anschluss die nachfolgenden Abfragen der Installation beantworten. Wir empfehlen bei allen Datenschutz- und Privatsphäre-Fragen immer die restriktivste Antwort zu wählen.

Nach der Installation den aktuellen Intelligent Hub (Dateiname „AirwatchAgent.msi“) von der Website <https://getwsone.com> herunterladen:



Die Software auf dem Endgerät mit den Standardeinstellungen installieren.



Hinweis: Ggf. taucht die UAC-Abfrage dabei minimiert auf:



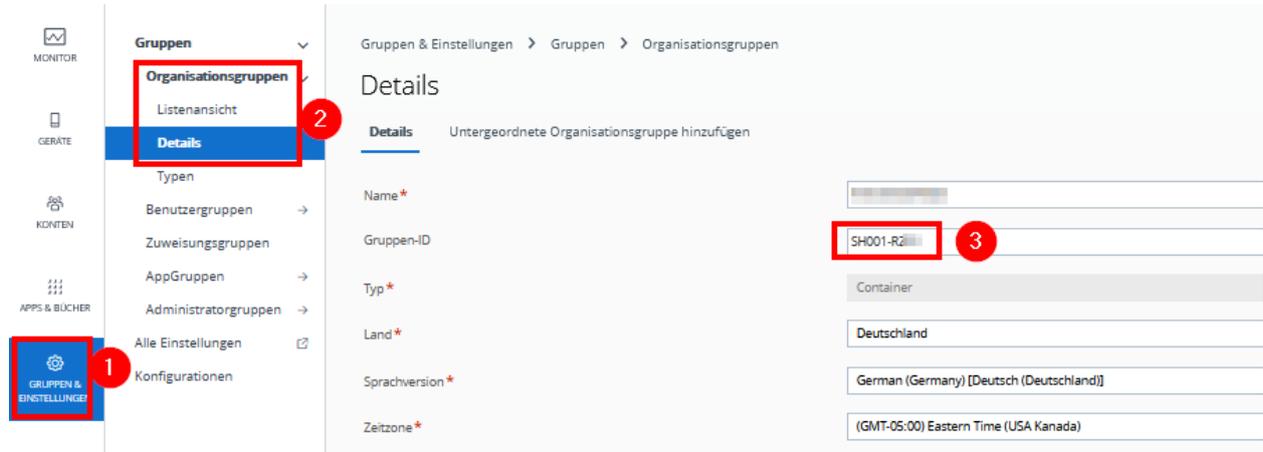
Nach der Installation startet der Intelligent Hub automatisch. Fahren Sie nun im nachfolgenden Kapitel fort.

4.1.3 Windows: Testgerät im UEM anmelden

Vor der UEM-Registrierung des Gerätes im Intelligent Hub benötigen Sie zunächst die Gruppen-ID des Schulträgers. Wechseln Sie dazu ins UEM und wählen oben am Bildschirmrand die Ebene des Schulträgers aus:

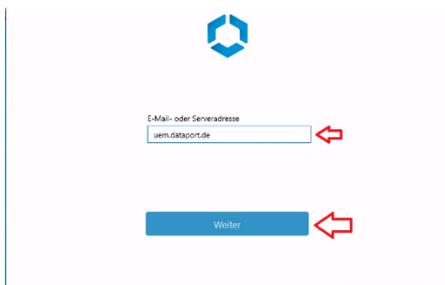


Die Gruppen-ID des Schulträgers (3) finden Sie unter dem Menüpunkt „Gruppen & Einstellungen“ (1) – „Gruppen“ – „Organisationsgruppen“ – „Details“ (2):

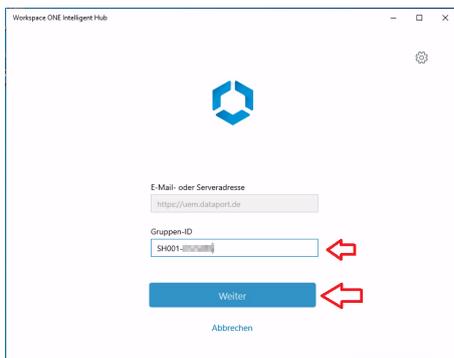


Hinweis: Die Gruppen-ID eines Schulträgers setzt sich aus dem Prefix „SH001“ dem Kreis-Kennzeichen und einer Nummer zusammen.

Im Anschluss auf dem Endgerät den Intelligent Hub starten, als Serveradresse *uem.dataport.de* eingeben und mit „Weiter“ bestätigen:



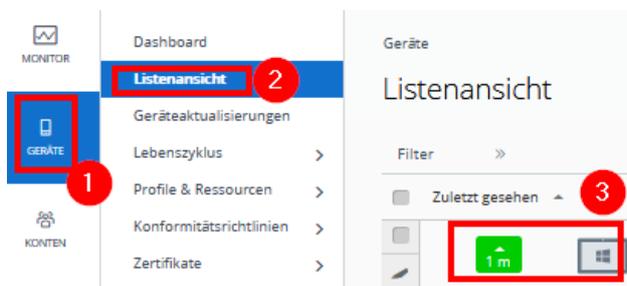
Die oben ermittelte Gruppen-ID des Schulträgers eingeben:



Im letzten Schritt die Anmeldedaten des Basic-Accounts (siehe oben) eingeben und mit „Anmelden“ bestätigen:



Nach erfolgter Anmeldung sollte im UEM unter „Geräte“ (1) – „Listenansicht“ (2) nun das Gerät (3) zu sehen sein:



Hinweise:

- Die Einrichtung von Einstellungen (Installation Profile, Bitlockerverschlüsselung etc.) und die Installation Software startet unmittelbar nach erfolgreicher Anmeldung. Lassen Sie das Gerät bitte angeschaltet und mit dem Internet verbunden. Je nach Gerät und Internet-Verbindung kann der Vorgang zwischen etwa 30 Minuten und einigen Stunden dauern. Unterbrechen Sie den Vorgang nach Möglichkeit nicht, da nicht unmittelbar zu erkennen ist, welche Aktionen im Hintergrund ablaufen.
- Obwohl auf dem Testgerät dieselben Richtlinien und Apps wie auf den Endgeräten für Lehrkräfte installiert wurden, kann es sein, dass das Startmenü anders aussieht. Hier tauchen ggf. noch Apps auf, die auf den LK-Endgeräten bereits vor der UEM-Anbindung deinstalliert waren.
- Spätestens nach der Rückkehr aus dem Standby-Modus bzw. nach einem Neustart werden Sie aufgefordert ein neues Kennwort zu vergeben. Sollten Sie zu Beginn des Prozesses kein Kennwort vergeben haben, so lassen Sie das Feld für das alte Kennwort leer. Geben Sie Ihr neues Kennwort in die zwei unteren Felder ein und bestätigen die Eingabe dann die "Enter-Taste" (Kennwort-Richtlinien: mindestens acht Zeichen, mindestens eine Zahl und ein Sonderzeichen):



4.2 iPadOS: Einbinden von Testgeräten

Das einzubindende Test-iPad muss folgende Voraussetzungen erfüllen:

- Einbindung in die Geräteverwaltung des schulträgereigenen Apple School Managers
- keine Zuordnung zu einem anderen Mobile-Device-Mangement-System (MDM)
- Installation des aktuellen Betriebssystems (iPadOS 15 und neuer)
- Zurücksetzung auf Werksteinstellungen

4.2.1 Anbindung des Apple School Managers für die Geräteregistrierung

Um Test-iPads im UEM registrieren zu können, muss der Apple School Manager (ASM) des Schulträgers einmalig an das UEM angebunden werden. Sollte noch kein Zugang ASM-Zugang vorhanden sein, muss dieser zunächst bei Apple (<https://school.apple.com/#enrollment>) beantragt werden.



Bei der Anbindung des Apple School Managers an das UEM sind zwei Varianten möglich:

- Variante 1 (empfohlen): Es wird im ASM lediglich ein Geräte-Standort (MDM-Sever) für den Schulträger angelegt. Test-iPads werden dann vom ASM automatisch der Schulträgerebene im UEM zugeordnet und können bei Bedarf nachträglich im UEM einer Schule zugeordnet werden.
Wichtig: Das Anbinden des Schulträgerstandortes an die Schulträgerebene im UEM ist erst möglich, wenn ein UEM-Account für diese Ebene vorliegt. Bei Schulträgern mit mehreren Schulen wird dieser Account erst freigeschaltet, wenn Auftragsverarbeitungsverträge aller Schulen vorliegen.
- Variante 2: Es wird ein Gerätestandort (MDM-Server) im ASM für jede Schule sowie ein Standort für den Schulträger angelegt. Test-iPads können bereits im ASM einzelnen Schulen zugewiesen werden. Diese tauchen im UEM dann nur in der zugehörigen Schulebene auf. Diese Variante ist z. B. dann sinnvoll, wenn unterschiedliche Schulen von unterschiedlichen Dienstleistern/Administratoren betreut werden und eine schulgenaue Zuweisung von Test-iPads schon im Apple School Manager benötigt wird.

Folgende Schritte müssen für die einmalige Anbindung des Apple School Managers an das UEM durchgeführt werden:

Zunächst ins UEM (<https://uem-console.dataport.de>) einloggen.

Dort die passende Organisationseinheit (z. B. Schulträger) auswählen:



Hinweis: Bei der Nutzung der Variante 1 (siehe oben) ist hier die Schulträgerebene zu wählen.

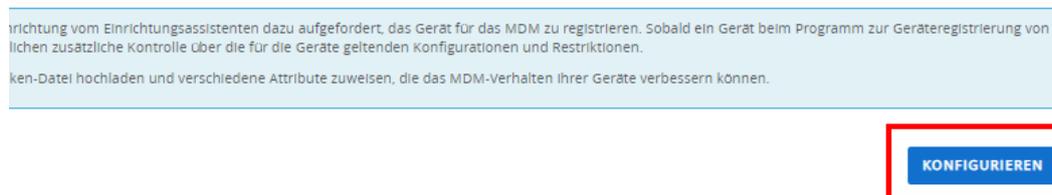
Im Menü „Geräte“ (1) – „Geräteeinstellungen“ (2) wählen:



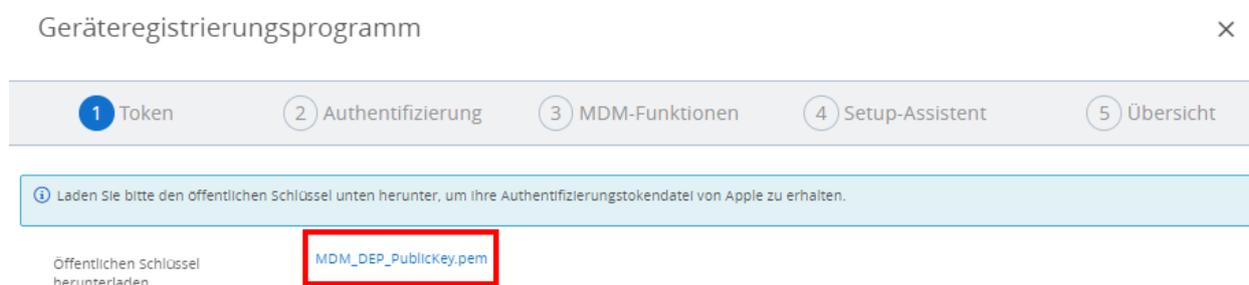
Im Anschluss „Apple“ – „Geräteregistrierungsprogramm“ (1) auswählen und für „Aktuelle Einstellung“ die Option „Überschreiben“ (2) aktivieren:



Mit „Konfigurieren“ bestätigen:

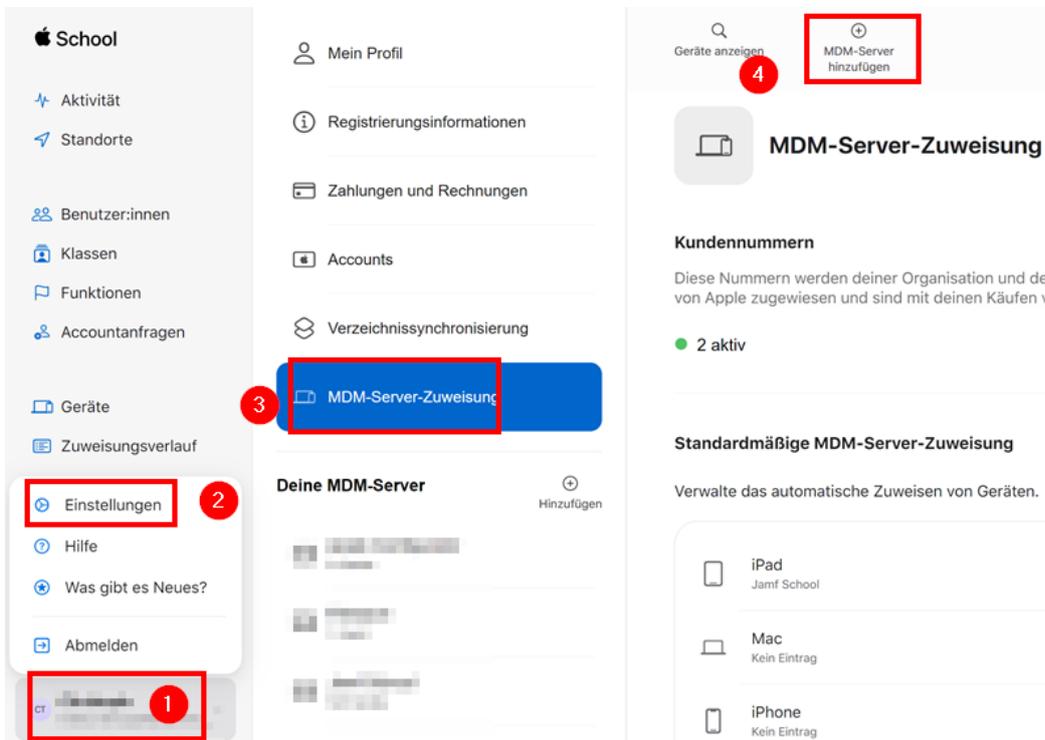


Den öffentlichen Schlüssel auf das eigene Endgerät herunterladen:

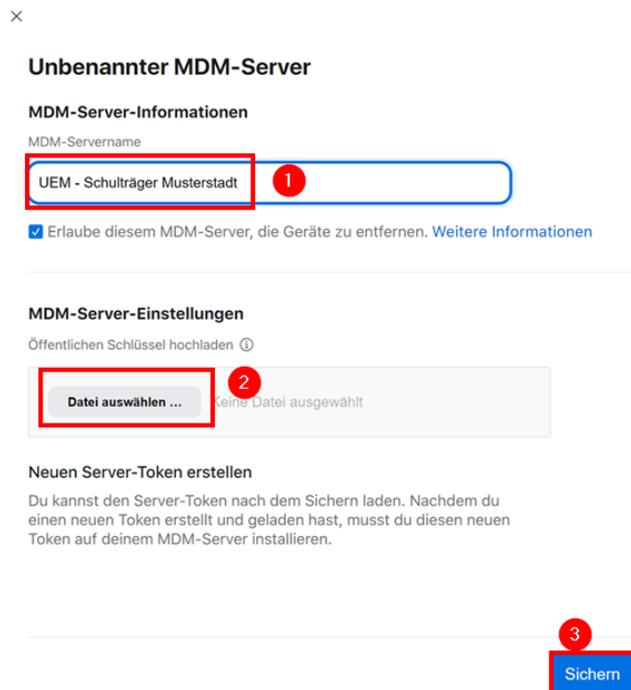


Das UEM-Browserfenster geöffnet lassen und in einem weiteren Browserfenster in den Apple School Manager (<https://school.apple.com>) einloggen.

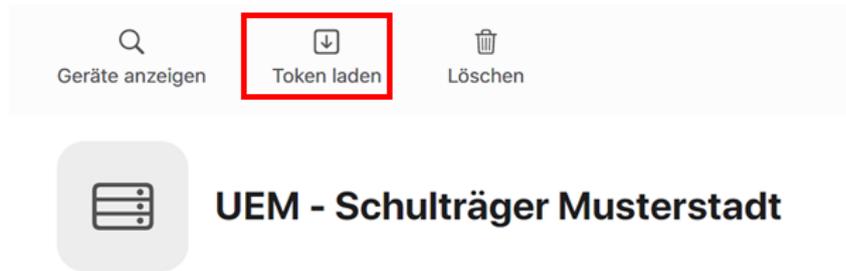
Im Menü den eigenen Kontonamen (1), „Einstellungen“ (2) – „MDM-Server-Zuweisung“ (3) – „MDM-Server hinzufügen“ (4) wählen:



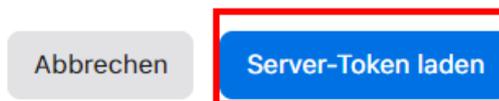
Einen passenden Servernamen (z. B. „UEM – Schulträger Musterstadt“) eingeben (1), den oben heruntergeladenen öffentlichen Schlüssel über „Datei auswählen...“ (2) in den Apple School Manager hochladen und mit „Sichern“ (3) bestätigen:



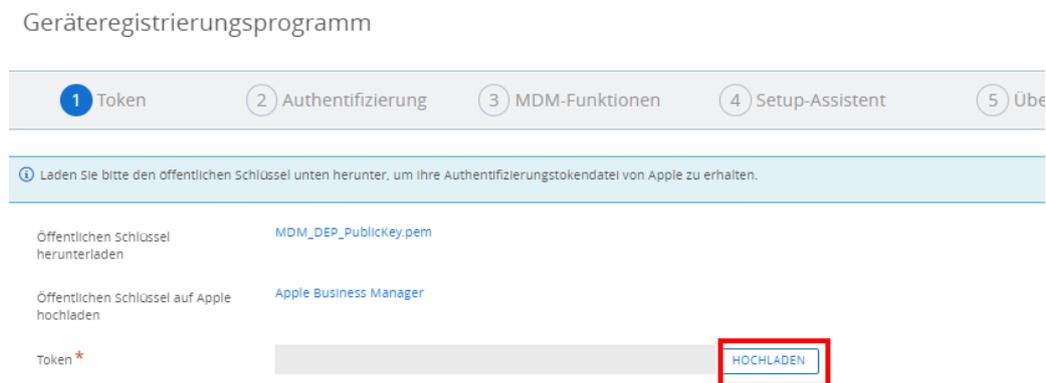
Im Anschluss werden die Einstellungen des neuen MDM-Servers angezeigt. Hier über „Token laden“ den Server-Token auf das eigene Endgerät herunterladen:



Im Anschluss mit „Server-Token laden“ bestätigen:



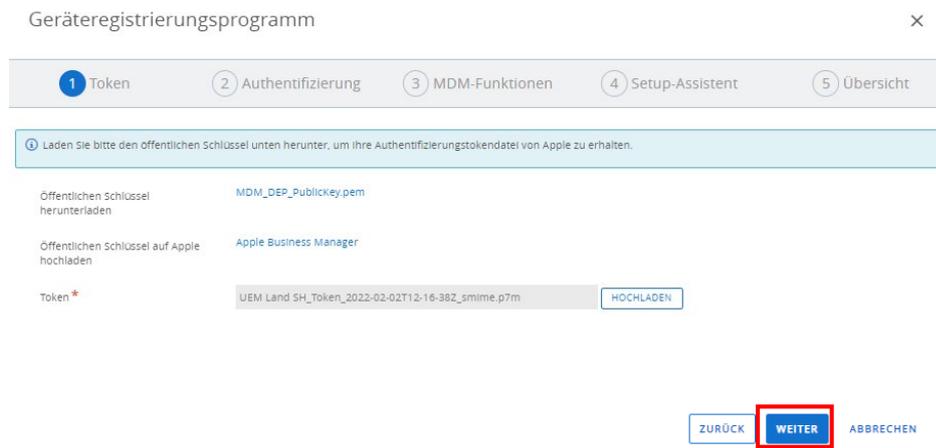
Zurück ins UEM wechseln und dort unter „Token“ den Button „Hochladen“ wählen:



Den eben vom Apple School Manager heruntergeladenen Server-Token auswählen (1) und mit „Speichern“ (2) bestätigen:



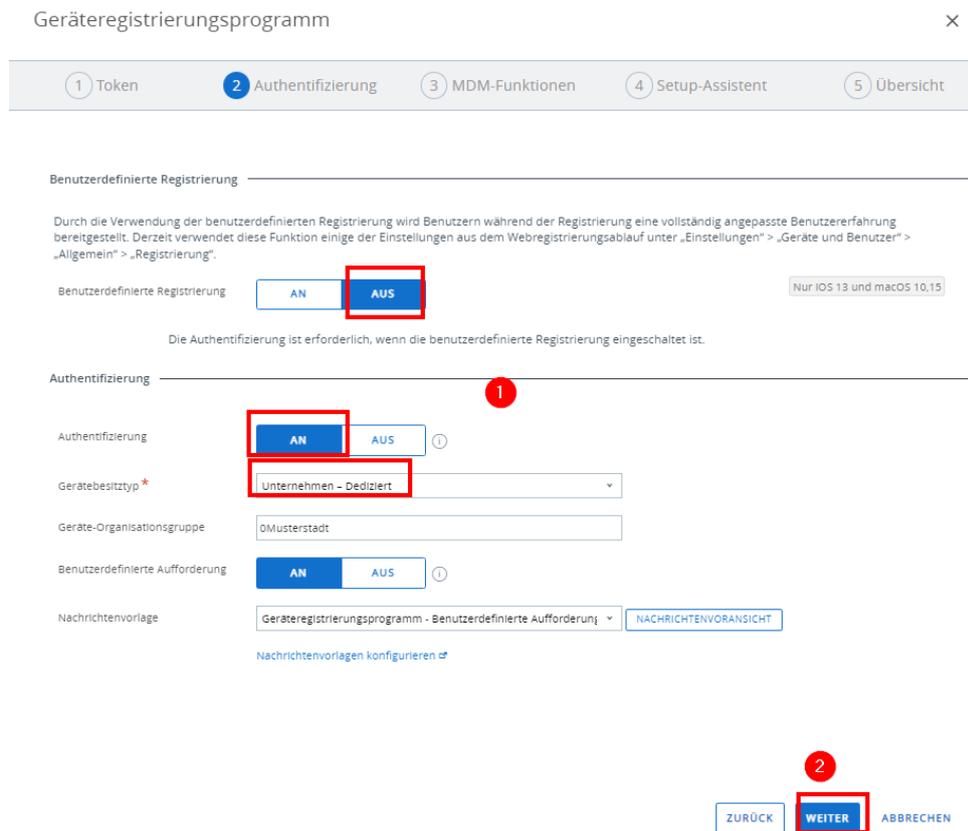
Im Anschluss mit „Weiter“ die Konfiguration fortsetzen:



Im nächsten Schritt („Authentifizierung“) die folgenden Optionen einstellen (1):

- Benutzerdefinierte Registrierung: „AUS“
- Authentifizierung: „AN“
- Gerätebesitztyp: „Unternehmen – Dediziert“

Alle weiteren Optionen in der Voreinstellung belassen und mit „Weiter“ (2) bestätigen:



Im dritten Schritt („MDM-Funktionen“) die Pflichtfelder ausfüllen (1). Dabei einen passenden Profilenames (z. B. „SH001“ + Name des Schulträgers) vergeben. Die Eingabe für „Abteilung“ (z.

B. „IT-Support“ + Schulträgername) und „Supportnummer“ (z. B. die Telefonnummer des IT-Supports) kann frei gewählt werden. Beide Informationen werden später bei der Anmeldung des Test-iPads unter den Details zur entfernten Verwaltung angezeigt. Die weiteren Optionen (2) können in der Voreinstellung belassen werden. Mit „Weiter“ bestätigen (3):

Gerätregistrierungsprogramm ×

1 Token 2 Authentifizierung **3 MDM-Funktionen** 4 Setup-Assistent 5 Übersicht

1 MDM-Profil und Geräteeigenschaften definieren

Profilname *

Abteilung * **1**

Supportnummer *

MDM-Registrierung erforderlich AKTIVIERT DEAKTIVIERT ⓘ

Überwachung AKTIVIERT DEAKTIVIERT ⓘ

MDM-Profil sperren AKTIVIERT DEAKTIVIERT ⓘ

Ankerzertifikat AKTIVIERT DEAKTIVIERT ⓘ

Gerätekopplung AKTIVIERT DEAKTIVIERT ⓘ **2**

Zertifikat der Überwachungsidentität ✕

Konfiguration abwarten AKTIVIERT DEAKTIVIERT ⓘ

Einrichtung der automatischen Weiterleitung AKTIVIERT DEAKTIVIERT ⓘ

Nur iOS 12.4 und darunter

Nur iOS 12.4 und darunter

Nur iOS 12.4 und darunter

Nur iOS

3 Nur macOS und tvOS

Die Einstellungen für Schritt 4 („Setup-Assistent“) können wie voreingestellt übernommen (1) und mit „Weiter“ (2) bestätigt werden:

Geräteregistrierungsprogramm ×

1 Token
 2 Authentifizierung
 3 MDM-Funktionen
 4 Setup-Assistent
 5 Übersicht

i Deaktivieren Sie folgende Optionen, sodass der Benutzer während der Ersteinrichtung des Geräts vom Assistenten keine Eingabeaufforderungen erhält. Wird dies übersprungen, wird für diese bestimmte Option die Standardeinstellung „Deaktiviert“ ausgewählt.

Kennung	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	Nur iOS
Biometrische ID	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Ortungsdienste	<input type="button" value="ÜBERSPRINGEN"/> <input checked="" type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Wiederherstellung aus der Sicherung	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Wiederherstellung abgeschlossen	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	Nur iOS
Von Android verschleiben	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	Nur iOS
Mit Apple ID und iCloud anmelden	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Nutzungsbedingungen und Bedingungen	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Siri	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Diagnose	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	
Registrierung	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	Nur macOS
Apple Pay	<input checked="" type="button" value="ÜBERSPRINGEN"/> <input type="button" value="NICHT ÜBERSPRINGEN"/> 1	

ZURÜCK
WEITER
ABBRECHEN

Im abschließenden Schritt („Übersicht“) die Optionen „Jetzt synchronisieren und an alle Geräte zuweisen“ sowie „Standardprofil automatisch zuweisen“ auf „JA“ stellen (1) und mit „Speichern“ (2) das Profil anlegen:

Geräteregistrierungsprogramm ×

1 Token 2 Authentifizierung 3 MDM-Funktionen 4 Setup-Assistent **5 Übersicht**

Jetzt synchronisieren und an alle Geräte zuweisen JA NEIN ⓘ 1

Standardprofil automatisch zuweisen JA NEIN ⓘ

Authentifizierung

Authentifizierung: An

Gerätebesitztyp: Unternehmen – Dediziert

Geräte-Organisationsgruppe: 0Musterstadt

Aufforderung anpassen: An

Nachrichtenvorlagen-ID: Geräteregistrierungsprogramm - Benutzerdefinierte Aufforderung@C

MDM-Funktionen

Profilname: SH001-Musterstadt

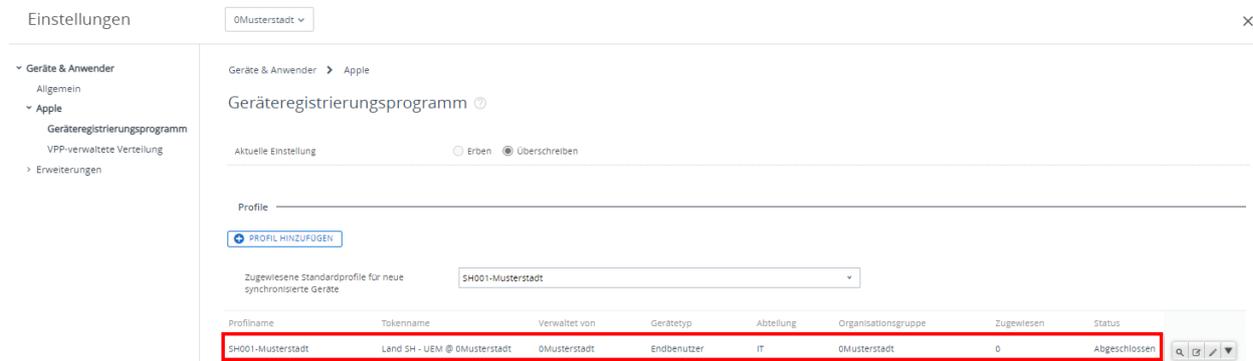
Abteilung: IT-Support

Supportnummer: 0431-12345678910

.....

ZURÜCK
SPEICHERN
ABBRECHEN

Im Anschluss wird das erstellte Profil angezeigt (unter „Apple“ – „Geräteregistrierungsprogramm“):

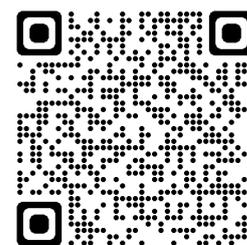


Hinweis: Wenn das erstellte Profil auf Schulträgererebene angelegt wurde und auch für die Schulen eigene MDM-Standorte angelegt werden sollen, muss in der Profilsicht die Option „Berechtigung für untergeordnete Elemente“ auf „Erben oder überschreiben“ (1) umgestellt und im Anschluss mit „Speichern“ (2) bestätigt werden:



4.2.2 iPad dem UEM zuweisen

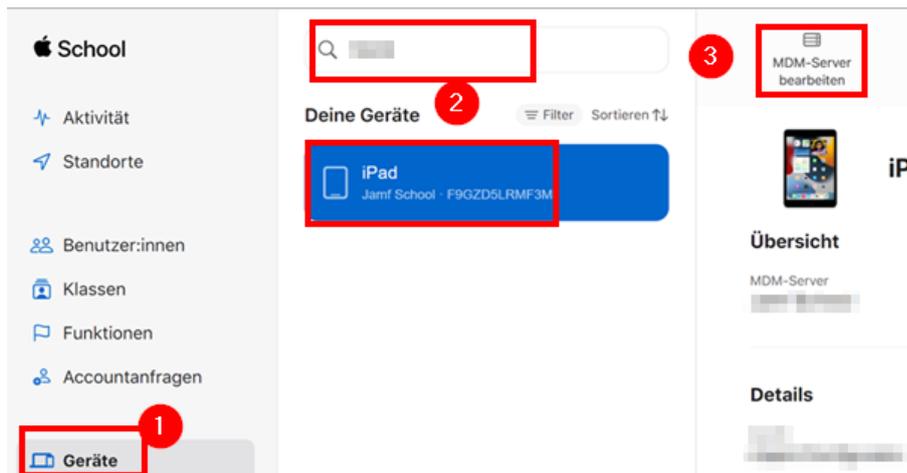
Hinweis: Um ein Test-iPad in die UEM-Verwaltung zu bringen, muss es bereits im Vorfeld im Apple School Manager (ASM) registriert worden sein. Dies geschieht im Normalfall über das Geräteregistrierungsprogramm von Apple (DEP), über das der Händler, bei dem das iPad erworben wurde, diese Zuweisung vor dem Kauf durchführt. Nachträglich lassen sich iPads nur manuell registrieren. Dazu wird ein Mac-Rechner mit der aktuellen Version des Apple Configurators 2 (ab Version 2.5) benötigt. Die Einrichtung wird u.a. hier erklärt: <https://help.apple.com/configurator/mac/2.7/#/cad99bc2a859>.



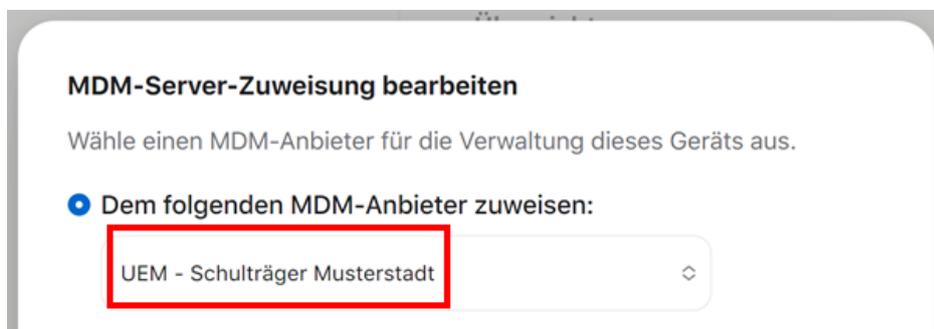
Folgende Schritte müssen für die Zuweisung des Test-iPads zum UEM vorgenommen werden:

In den Apple School Manager (<https://school.apple.com>) einloggen.

Im Menü unter „Geräte“ (1) das Test-iPad (ggf. über die Eingabe der Seriennummer) suchen und auswählen (2). Im Anschluss „MDM-Server bearbeiten“ (3) anklicken:



Den oben eingerichteten MDM-Server für das UEM des Landes auswählen und mit „Weiter“ bestätigen:



Die Gerätezuweisung mit „Bestätigen“ abschließen:



Möchtest du wirklich den MDM-Server ändern, der diesem Gerät zugewiesen ist?

Änderungen in der Zuweisung werden übernommen, wenn das Gerät das nächste Mal die automatische Geräteregistrierung im Konfigurationsassistenten verwendet.

Abbrechen

Bestätigen

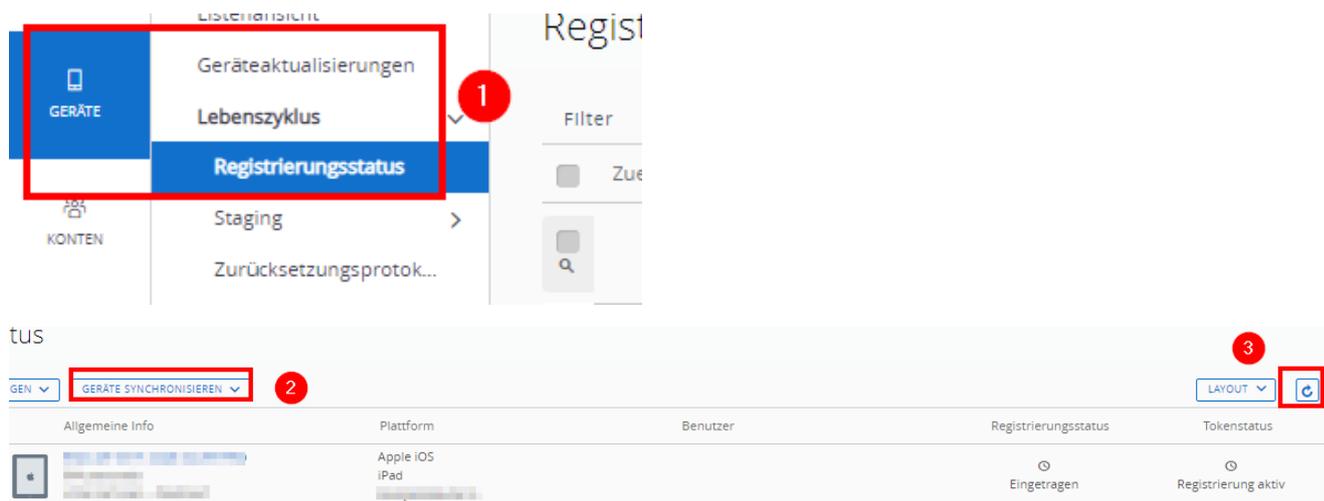
Hinweis: Bevor das Test-iPad ins UEM eingebucht werden kann, muss zunächst die Gerätesynchronisierung zwischen dem Apple School Manager und dem UEM stattgefunden haben. Dies wird einmal täglich automatisiert durchgeführt bzw. kann manuell sofort angestoßen werden.

Dazu zurück ins UEM (<https://uem-console.dataport.de>) wechseln.

Dort zunächst in die Organisationseinheit (Schule bzw. Schulträger) wechseln:



Im Menü „Geräte“ – „Lebenszyklus“ – „Registrierungsstatus“ (1) wählen. Im Anschluss dort den Menüpunkt „Geräte synchronisieren“ (2) sowie „Apple“ und „Synchronisieren“ wählen und nach kurzer Zeit das Pfeil-Symbol (3) zum Aktualisieren der Liste anklicken:



Das Test-iPad sollte nun in der Liste auftauchen.

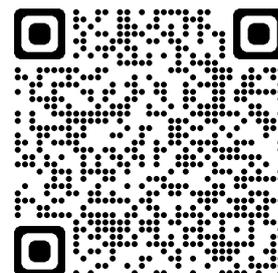
Hinweis: Alternativ kann die Synchronisierung auch über die Menüpunkte „Geräte“ – „Geräteeinstellungen“ – „Apple“ – „Geräteregistrierungsprogramm“ und den Button „Alle Geräte abrufen“ erfolgen.

4.2.3 iPad im UEM anmelden

Wenn noch nicht geschehen: das Test-iPad über die Einstellungen manuell zurücksetzen („Allgemein“ – „iPad übertragen/zurücksetzen“ - „Alle Inhalte und Einstellungen löschen“).

Das iPad starten und die Einrichtung wie in der Anleitung zur Ersteinrichtung für Lehrkräfte-iPads beschrieben durchführen:
<https://medienberatung.igsh.de/endgeraete-ik-s-anl-videos.html>.

Wichtig: Für die Anmeldung (Schritt 8) die Zugangsdaten des Basic-Accounts (siehe oben) nutzen.



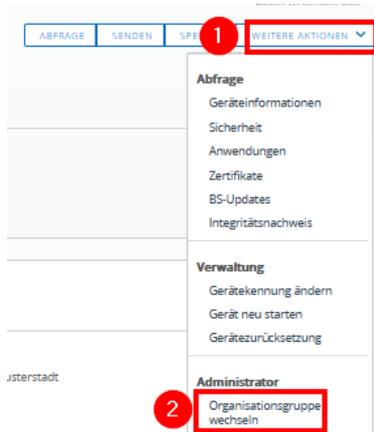
4.3 Windows und iPadOS: Testgeräte im UEM verschieben

Sie können ein Testgerät innerhalb der Schulträger-Ebene zu einer zugehörigen Schule bzw. zurück auf die Schulträger-Ebene verschieben.

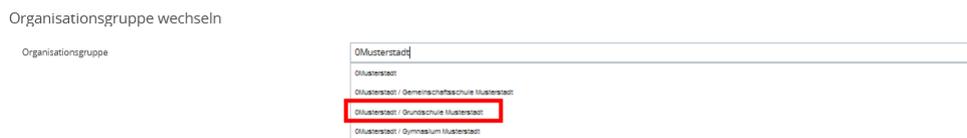
Zunächst in die Organisationseinheit des Schulträgers wechseln:



Die Detailansicht des entsprechenden Gerätes unter „Geräte“ – „Listenansicht“ und wählen unter „Weitere Aktionen“ (1) die Schaltfläche „Organisationsgruppe wechseln“ (2):



Im Anschluss die neue Organisationsgruppe (Schule) auswählen:



Hinweis: Sollte nur eine Schule sichtbar sein, muss der voreingetragene Text unter „Organisationsgruppe“ entfernt werden.

Mit „Speichern“ bestätigen.

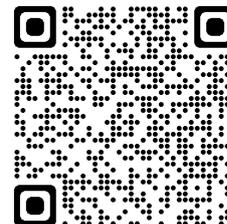
In der Detailansicht des Gerätes unter „Geräteinformationen“ sollte nun die neue Organisationsgruppe auftauchen:



4.4 Windows und iPadOS: Testgerät aus dem UEM entfernen

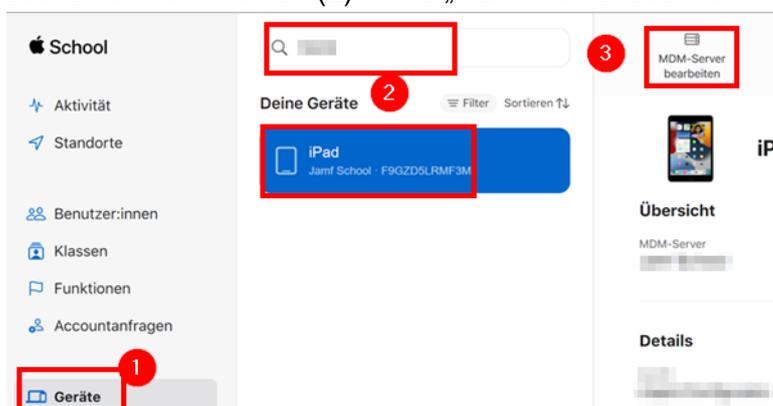
Um ein Testgerät (iPadOS oder Windows) bei Bedarf wieder aus dem UEM zu entfernen, muss dieses durch den Dataport-Support zurückgesetzt werden und aus dem UEM-gelöscht werden.

Geben Sie dazu ein Ticket über das Helpdesk-Formular unter <https://www.secure-lernnetz.de/helpdesk> im Bereich „LK-Endgeräte“ – „Support“ mit Angabe der Geräte-Seriennummer und der zugehörigen Organisationsgruppe (Schule bzw. Schulträger) auf.



Nach dem Löschen eines iPads aus dem UEM durch Dataport muss zusätzlich noch im Apple School Manager die Zuordnung zum Gerätestandort (MDM-Server) des UEM aufgehoben werden, damit über die Synchronisierung nicht erneut das Gerät dem UEM zugewiesen wird:

- In den Apple School Manager (<https://school.apple.com>) einloggen.
- Im Menü unter „Geräte“ (1) das Test-iPad (ggf. über die Eingabe der Seriennummer) suchen und auswählen (2) sowie „MDM-Server bearbeiten“ (3) anklicken:



- Dann „Zuweisung zum aktuellen MDM-Anbieter aufheben“ (1) wählen und mit „Weiter“ (2) bestätigen:

MDM-Server-Zuweisung bearbeiten

Wähle einen MDM-Anbieter für die Verwaltung dieses Geräts aus.

Dem folgenden MDM-Anbieter zuweisen:

Zuweisung zum aktuellen MDM-Anbieter aufheben

Abbrechen

- Falls noch keine Zurücksetzung des iPads erfolgt ist, dieses ggf. manuell am iPad nachholen („Allgemein“ – „iPad übertragen/zurücksetzen“ - „Alle Inhalte und Einstellungen löschen“).

4.5 Basic-Benutzer: Passwort zurücksetzen

Bei Bedarf kann das Passwort des durch Dataport angelegten Basic-Benutzers, der wie oben beschrieben lediglich für die Einbindung von Testgeräten benötigt wird, selbstständig geändert werden.

Dazu in der Benutzerliste den betreffenden Basic-Benutzer auswählen (1) und „Nachricht senden“ wählen (2):

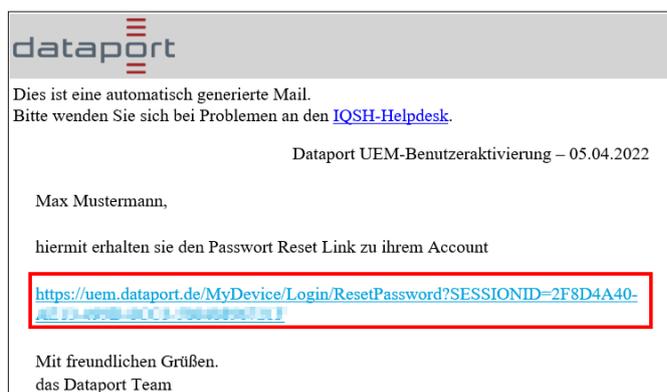


Im Anschluss „User PWD Reset Mail...“ (1) wählen und mit „Senden“ (2) bestätigen:

Nachricht senden (nur E-Mail)



Es wird nun an die hinterlegte Mailadresse ein Link gesendet, über den man ein neues Passwort für den Account des Basic-Benutzers vergeben kann:



5 Anlegen von Benutzergruppen

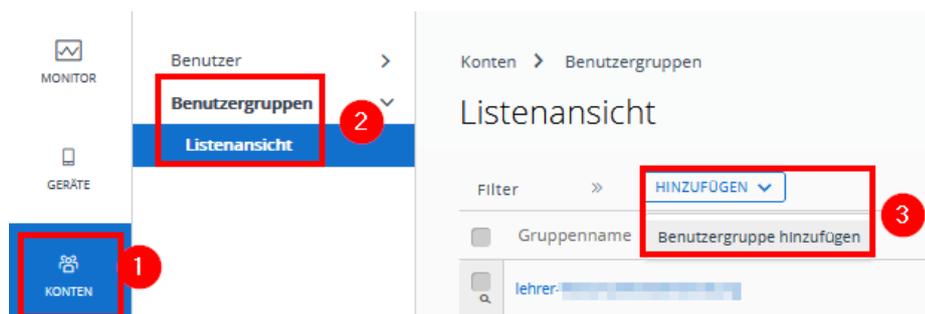
Für jede Schule ist bereits eine Benutzergruppen mit allen zur Schule gehörigen Lehrkräften angelegt. Der Name besteht aus „lehrer-“ und der Dienststellnummer der jeweiligen Schule. Die Benutzerdaten kommen aus dem Schulportal und werden einmal täglich von dort ins UEM hineinsynchronisiert.

Bei Bedarf können weitere Benutzergruppen (z. B. Fachschaftsgruppen) angelegt werden.

Zunächst die passende Organisationseinheit (z. B. eine Schule) wählen:



Dann im Menü „Konten“ (1) - „Benutzergruppen“ - „Listenansicht“ (2) - „Hinzufügen“ - „Hinzufügen von Benutzergruppen“ (3) wählen:



Als „Typ“ „Benutzerdefiniert“ wählen und den Gruppennamen nach Namensschema vergeben. Der Name soll aus den folgenden Bestandteilen GroupID (SH001), Bindestrich, Schulname, Gruppenname (zum Beispiel „SH001-GS Musterhausen Fachschaft Mathe“):

Benutzergruppe hinzufügen

Typ* VERZEICHNIS **BENUTZERDEFINIERT** 1

Gruppenname* 2

Beschreibung

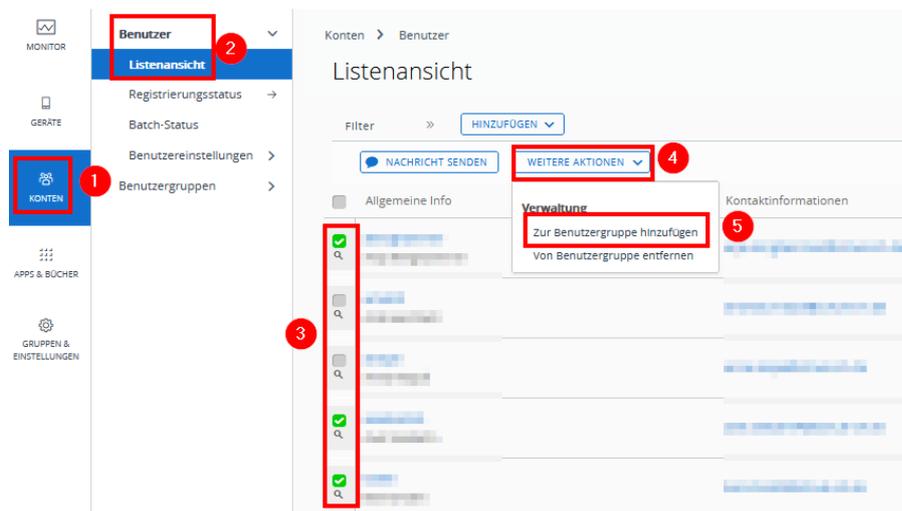
Verwaltet von

Hinweis: Ein nachträgliches Ändern eines Gruppennamens ist nicht möglich. Stattdessen müsste die zu ändernde Gruppe gelöscht und dann neu angelegt werden.

Mit „Speichern“ bestätigen.

Im Anschluss werden die zugehörigen Benutzer der Gruppe zugeordnet.

Dazu „Konten“ (1) - „Benutzer“ - „Listenansicht“ (2) wählen, die entsprechenden Benutzer markieren (3) und über „Weitere Aktionen“ (4) - „Zur Benutzergruppe hinzufügen“ (5) wählen:



Im Anschluss für „Bestehende Benutzergruppe“ (1) die oben angelegte Gruppe wählen:

Ausgewählte Anwender zur benutzerdefinierten Anwendergruppe hinzufügen



Mit „Speichern“ bestätigen.

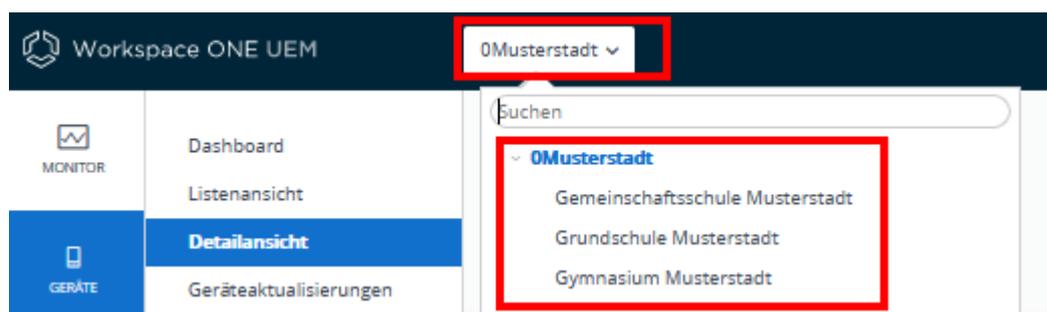
6 Anlegen von Zuweisungsgruppen (Smartgroups)

Mit Hilfe einer Zuweisungsgruppe (Smartgroup) lassen sich Apps und Profile einer bestimmten Zielgruppe zuweisen. Diese Gruppe kann entweder aus einzelnen Geräten und Benutzern oder aus einer vorher angelegten Benutzergruppe bestehen. Da Endgeräte an Schulportalnutzer gebunden sind, geht es hier in der Regel um eine benutzerbezogene Verteilung (einzelne Nutzer oder Benutzergruppen).

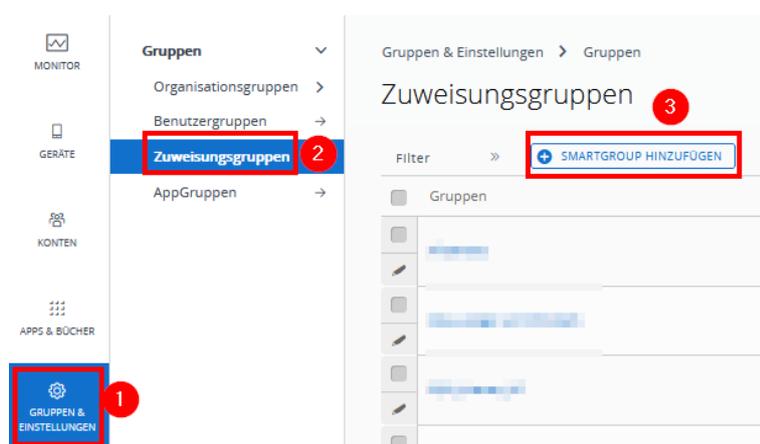
Empfehlenswert ist die Zuweisung zu einer vorhandenen Benutzergruppe (zum Beispiel alle Lehrkräfte einer Schule) oder zu einer neuangelegte Benutzergruppe (zum Beispiel eine Fachschaftsgruppe). Nur auf diesem Weg lassen sich bei Bedarf weitere Kriterien für die Verteilung festlegen, wie zum Beispiel das nachträgliche Hinzufügen oder Ausschließen von Personen.

Statt die Verteilung über eine Smartgroup zu organisieren, wäre auch eine direkte Verteilung an eine Organisationsgruppe möglich. Organisationsgruppen sind alle Geräte des jeweiligen Schulträgers bzw. der jeweiligen Schule. Nachteil: die Gruppe ist starr, eine flexible Einstellung (z. B. das nachträgliche Hinzufügen oder Ausschließen von Personen) ist hier nicht möglich.

Für das Erstellen einer Zuweisungsgruppe zunächst die passende Organisationseinheit (z. B. eine Schule) wählen:



Im Anschluss „Gruppen & Einstellungen“ - „Gruppen“ - „Zuweisungsgruppen“ - „Smartgroup hinzufügen“ wählen:

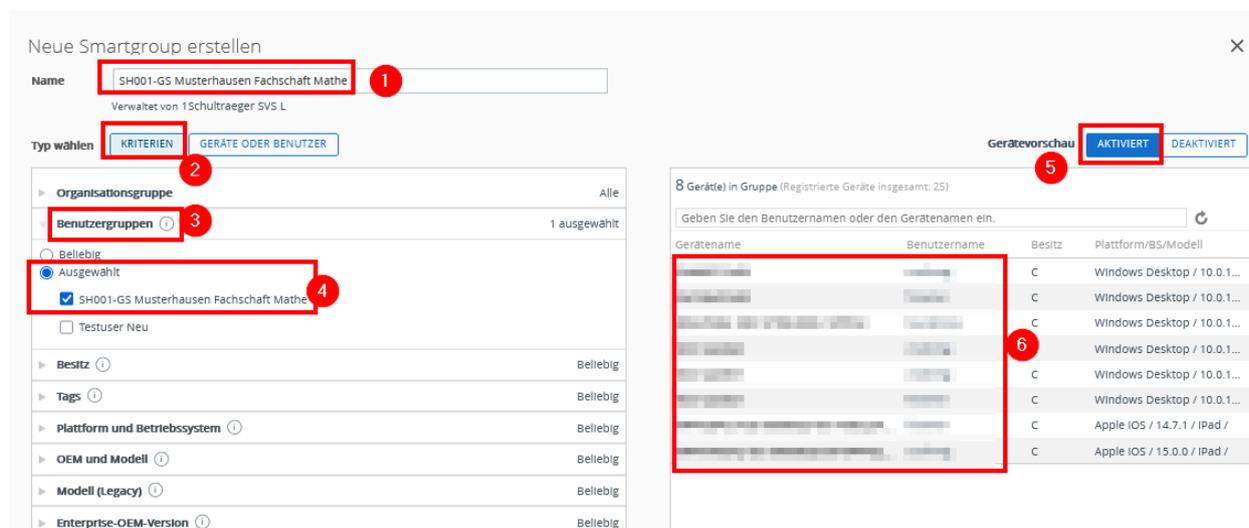


Im Anschluss den Namen der Zuweisungsgruppen nach Namensschema vergeben (1). Der Name soll aus den folgenden Bestandteilen GroupID (SH001), Bindestrich, Schulname,

Gruppenname (zum Beispiel „SH001-GS Musterhausen Fachschaft Mathe“): GroupID (SH001), Bindestrich, Schulname, Gruppenname (z.B. SH001-Musterschule Fachschaft Mathe).

Hinweis: Unter Zuweisungstyp unterscheidet man den Typ „Kriterien“ (Variante 1) vom Typ „Geräte oder Benutzer“ (Variante 2). Wir empfehlen hier die Nutzung der Variante 1. Diese basiert auf Benutzergruppen und lässt sich mit zusätzlichen Kriterien (z. B. Betriebssystem, Ausschlüsse) konfigurieren. Wenn eine Benutzergruppe ein neues Mitglied bekommt, erhält dieses automatisch alle Apps und Profile der entsprechenden Smartgroup. Dies wäre bei der Variante 2 nicht möglich. Dieser Typ empfiehlt sich nur bei einzelnen Benutzern bzw. Geräten, z. B. bei der Installation einer App auf einem Testgerät.

Variante 1 (empfohlen): Für „Typ“ „Kriterien“ auswählen (2), unter „Benutzergruppe“ (3) passende Gruppe(n) auswählen (4), ggf. die Gerätevorschau (5) aktivieren und Liste der Zielgeräte überprüfen (6):



Bei Bedarf weitere Kriterien zum Beispiel für die Punkte „Plattform und Betriebssystem“, „Hinzufügungen“, „Ausschlüsse“ ergänzen.

Mit „Speichern“ bestätigen.

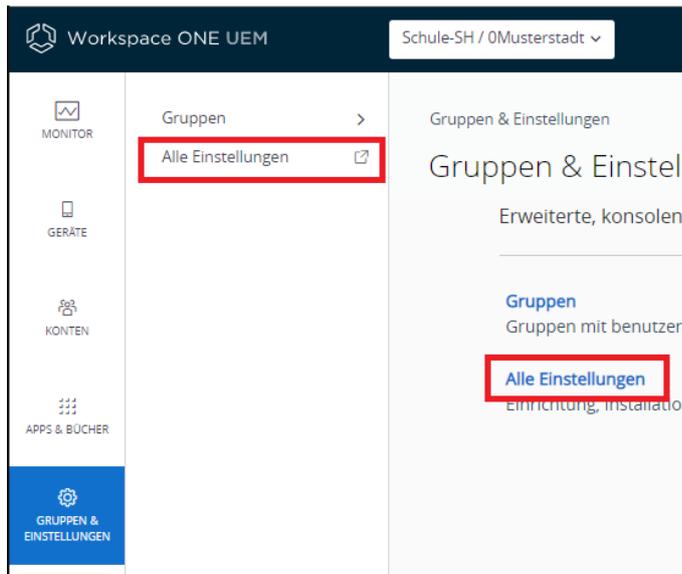
Variante 2: Als „Typ“ „Geräte oder Benutzer“ wählen. Einzelne Geräte oder Benutzer hinzufügen.

Mit „Speichern“ bestätigen.

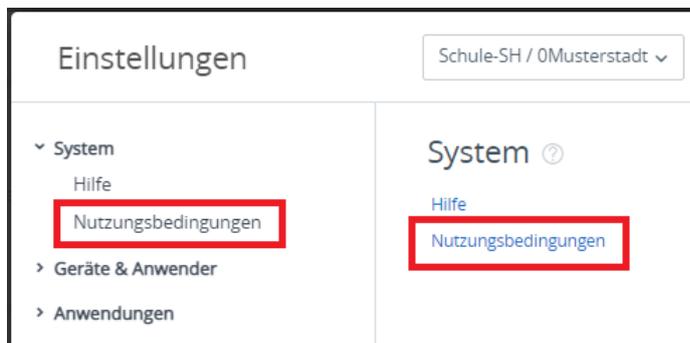
7 Anlegen von Nutzungsbedingungen

Nutzungsbedingungen sind einseitig vorformulierte Regelungen, mit der Nutzerinnen und Nutzer über ihre Rechte und Pflichten informiert werden. Die Bedingungen müssen vor Installation der App akzeptiert werden.

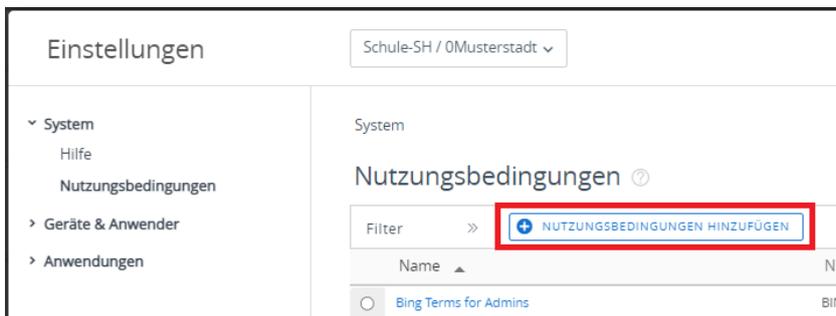
Nutzungsbedingungen werden im UEM in den Einstellungen verwaltet. Diese findet man unter „Gruppen und Einstellungen“. Beide angebotenen Links (siehe Grafik) führen dabei zur gleichen Ansicht der Einstellungen.



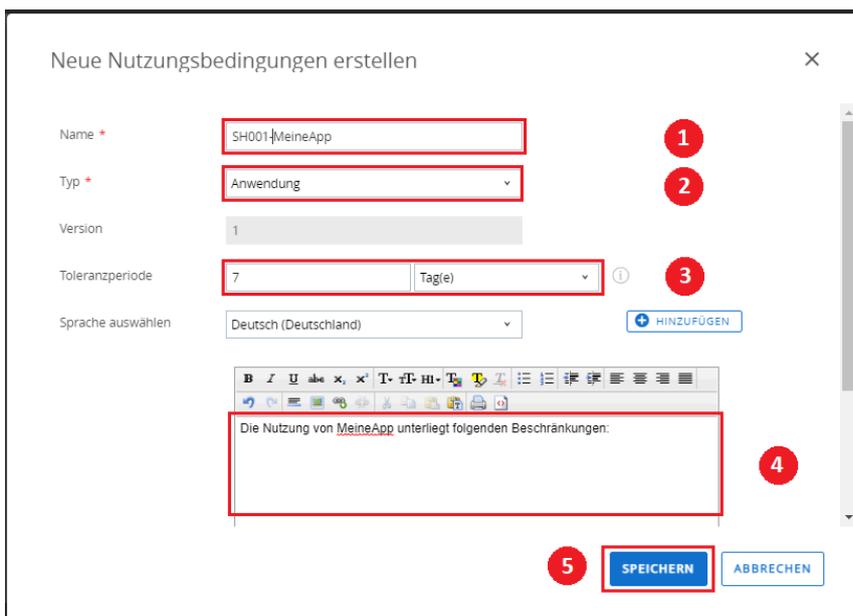
Die Nutzungsbedingungen finden sich im Bereich „System“. Auch hier führen beide Links zur gleichen Ansicht.



Die Anlage deiner neuen Nutzungsbedingung erfolgt über „NUTZUNGSBEDINGUNG HINZUFÜGEN“



Der Name der Nutzungsbedingung (1) sollte entsprechend der Namenskonvention mit der GroupID SH001 inkl. Bindestrich beginnen. Nach Festlegung des Namens ist der Typ (2) zu wählen, wobei es in der genutzten Systemkonfiguration nur die Option „Anwendung“ gibt. Die Toleranzperiode gibt den Zeitraum an, innerhalb derer die Nutzungsbedingung durch Nutzerinnen und Nutzer akzeptiert werden muss. Andernfalls wird die App entfernt. Die Beschreibung der Nutzungsbedingung erfolgt im darunterliegenden Textfeld (4). Mit „Speichern“ (5) werden die Einstellungen gesichert und die Nutzungsbedingung aktiviert.

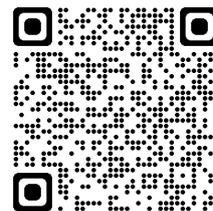


Die Nutzungsbedingung kann anschließend in der Detailansicht der App hinterlegt werden. Nach Speicherung erfolgt die Aktualisierung der Zuweisung.

Hinweis: Nach Aktualisierung einer Nutzungsbedingung einer App muss diese erneut von den Nutzerinnen und Nutzern akzeptiert werden. Andernfalls wird die App nach Verstreichen der Toleranzperiode gelöscht. Der Aufruf der Nutzungsbedingungen erfolgt durch Klick auf „Installation“ im Hub. Nach Bestätigung der Bedingungen wird die Installation der App jedoch übersprungen.

8 iPadOS: Anbindung des Apple School Managers für die App-Verteilung

Um Apps auf iPads verteilen zu können, muss zunächst der vorhandene Zugang des Schulträgers zum Apple School Manager (ASM) an das UEM des Landes angebunden werden. Sollte noch kein Zugang ASM-Zugang vorhanden sein, muss dieser zunächst bei Apple (<https://school.apple.com/#enrollment>) beantragt werden.

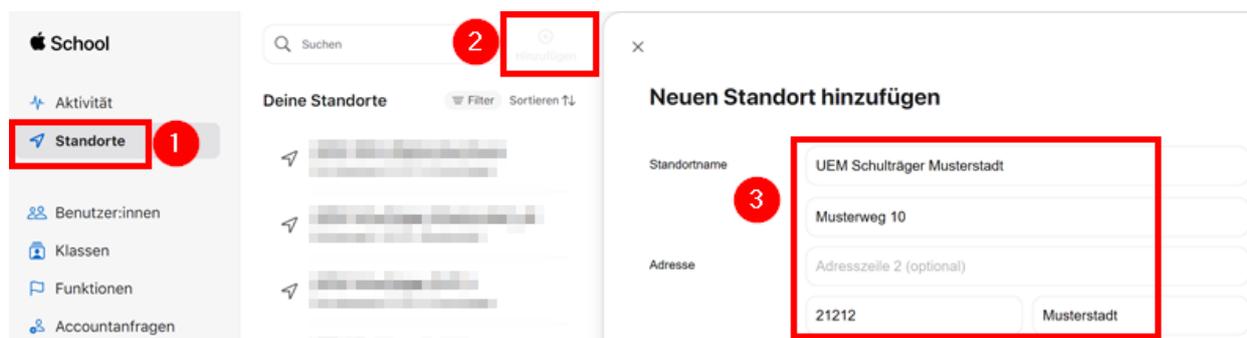
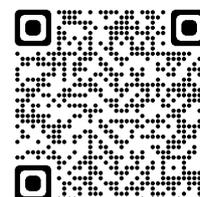


Im Apple School Manager wird/werden zunächst (ein) Standort(e) für das UEM des Landes angelegt und zugehörige Server-Token generiert werden. Zwei Varianten sind dabei möglich:

- Variante 1 (empfohlen): Es wird lediglich ein Standort für den Schulträger im ASM angelegt. Apps werden auf Schulträgerebene gekauft und später im UEM den jeweiligen Schulen zugeordnet.
Wichtig: Das Anbinden des Schulträgerstandortes an die Schulträgerebene im UEM ist erst möglich, wenn ein UEM-Account für diese Ebene vorliegt. Bei Schulträgern mit mehreren Schulen wird dieser Account erst freigeschaltet, wenn Auftragsverarbeitungsverträge aller Schulen vorliegen.
- Variante 2: Es werden Standorte für jede Schule und den Schulträger im ASM angelegt. Apps können bereits im Apple School Manager einzelnen Schulen zugewiesen werden. Diese tauchen im UEM dann nur in der zugehörigen Schulebene auf. Diese Variante ist z. B. dann sinnvoll, wenn unterschiedliche Schulen von unterschiedlichen Dienstleistern/Administratoren betreut werden und eine schulgenaue Zuweisung von Apps schon im Apple School Manager benötigt wird.

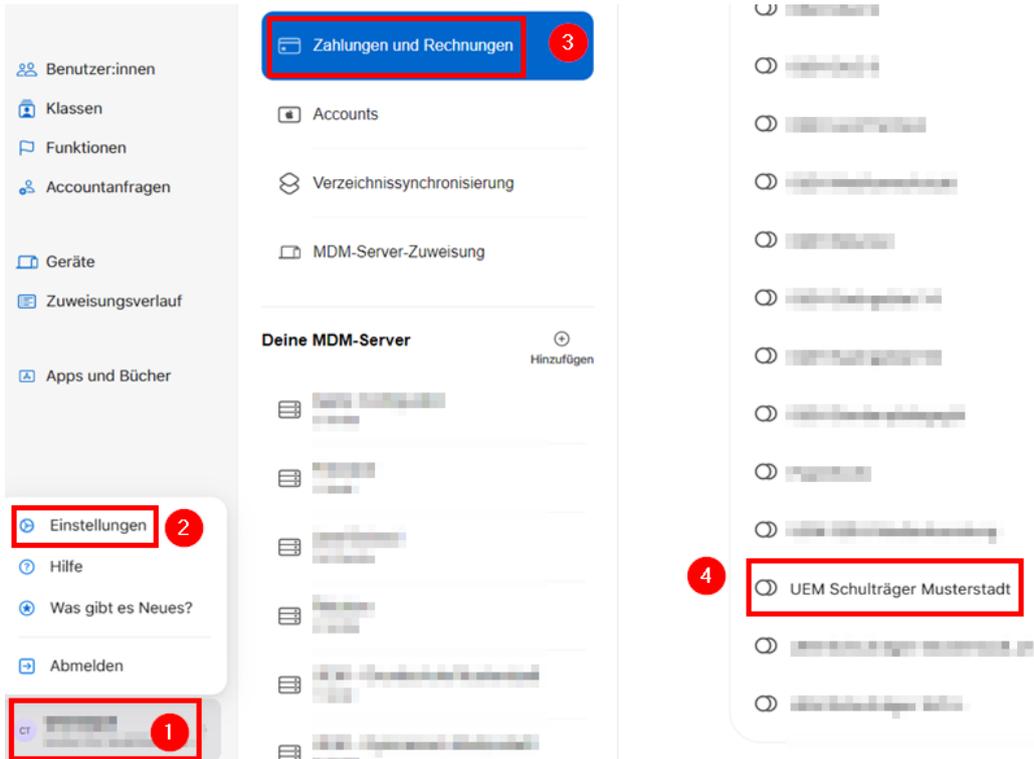
Zunächst in den Apple School Manager über <https://school.apple.com> einloggen.

Im Menü „Standorte“ (1) - „Hinzufügen“ (2) wählen, Standortnamen (z.B. „UEM Schulträger Musterstadt“) und Anschrift des Schulträgers (3) eingeben:



Mit „Sichern“ bestätigen.

Im Anschluss für den/die neuangelegten Standort(e) den/die zugehörigen Server-Token herunterladen. Dazu im Menü den eigenen Kontonamen (1), „Einstellungen“ (2) - „Zahlungen und Rechnungen“ (3) wählen und auf der rechten Seite in der Spalte „Server-Tokens“ den den neuangelegten UEM-Standort anklicken (4):



Nach dem Herunterladen der Servertoken ins UEM wechseln und dort im Menü „Geräte“ (1) und „Geräteeinstellungen“ (2) wählen:



Im Anschluss „Apple“ - „VPP-verwaltete Verteilung“ wählen (1), auf die Ebene der passenden Schule umstellen (2), „Überschreiben“ wählen (3), als Beschreibung ASM-Standortnamen und ggf. verwendete Apple-ID eingeben (4) und über „Hochladen“ den passenden Server-Token einstellen:

Einstellungen _Schulträger SVS L 2

▼ Geräte & Anwender

- Allgemein
- Apple 1
- VPP-verwaltete Verteilung 1
- Erweiterungen

Geräte & Anwender > Apple

VPP-verwaltete Verteilung ⊙

Aktuelle Einstellung Erben Überschreiben 3

Melden Sie sich bei Ihrem VPP-Speicher an, um das für die von VPP verwaltete Verteilung benötigte sToken aus Ihrer Kontoubersicht herunterzuladen.

Beschreibung * Musterhausen 4

sToken * HOCHLADEN 5

Einladungen automatisch senden ⊙

Nachrichtenvorlage NACHRICHTENVORANSICHT

E-Mail-Benachrichtigungen betreffen nur iOS-Geräte mit den Versionen iOS 7.0.0 bis iOS 7.0.2. Geräte, die iOS 7.0.3 und höher verwenden, erhalten Einladungen automatisch.

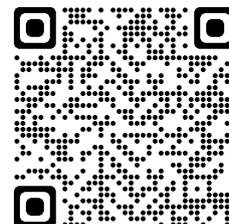
Zwei Mal mit „Speichern“ bestätigen.

9 iPadOS: App-Kauf, -Installation, -Deinstallation

9.1 App-Einkauf

Zunächst in den Apple School Manager über <https://school.apple.com> einloggen.

Unter „Apps und Bücher“ (1) die gewünschte App suchen (2), die App auswählen (3), den passenden Standort einstellen (4), die App-Anzahl festlegen (5) und mit „Laden“ (6) bestätigen:



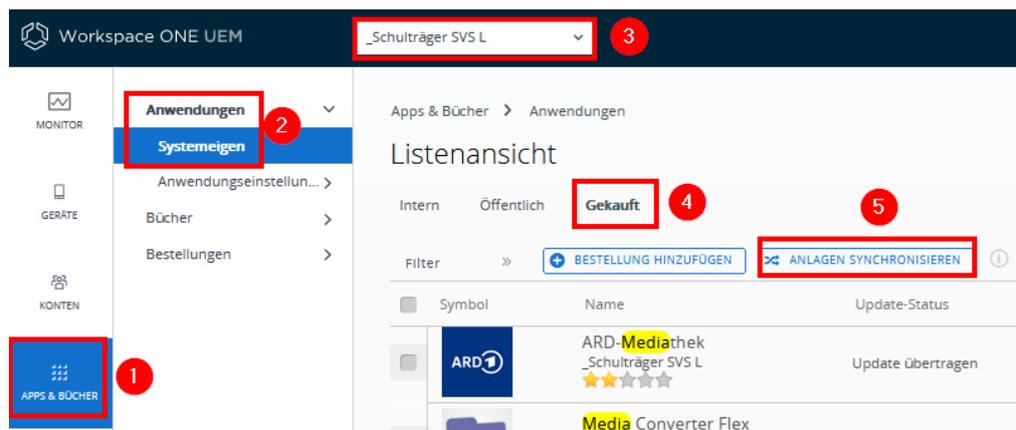
Nach kurzer Zeit taucht in den App-Details im Abschnitt „Lizenzen verwalten“ der Standort mit den zugewiesenen App-Lizenzen auf:

Lizenzen verwalten

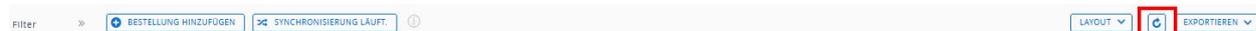
Standort	Im Einsatz	Verfügbar	
Papierkorb	0	150	Übertragen
UEM Schulträger Musterstadt	0	50	Übertragen
Gesamt	0	200	

Zusätzlich erhält man an die im ASM registrierte E-Mail-Adresse eine Bestätigungsnachricht zum App-Kauf.

Ins UEM wechseln, „Apps & Bücher“ (1) - „Anwendungen“ - „Systemeigen“ (2) anklicken, in die Übersicht der Schule bzw. des Schulträgers wechseln (3), den Reiter „Gekauft“ (4) und dort „Anlagen synchronisieren“ (5) wählen.



Etwa 10 Sekunden lang die Synchronisierung der Apps abwarten und dann über „Aktualisieren“ (Pfeil rechts zwischen „Layout“ und „Exportieren“) die Ansicht neu laden:

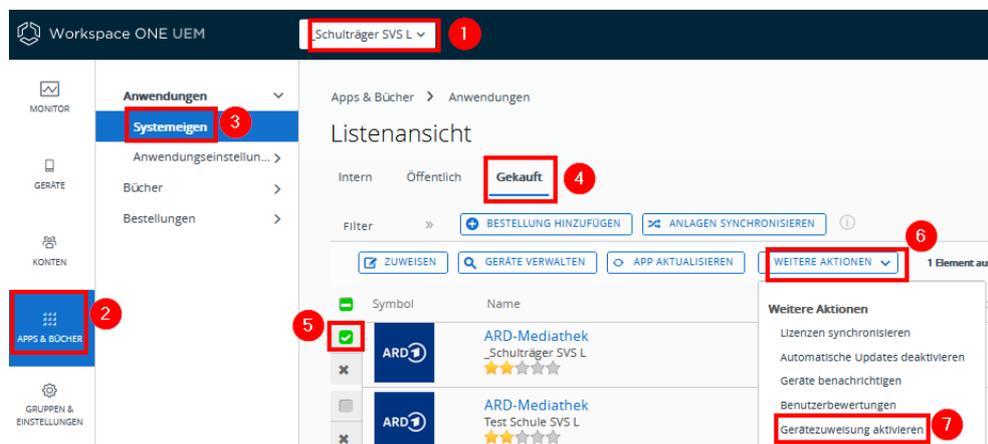


Die App sollte nun in der Appliste auftauchen.

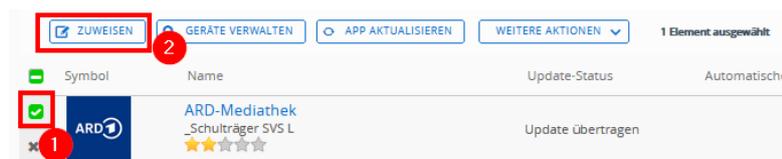
Hinweis: Falls die App nicht auftaucht, sollte die Synchronisierung und die Aktualisierung erneut durchgeführt werden.

9.2 App-Installation

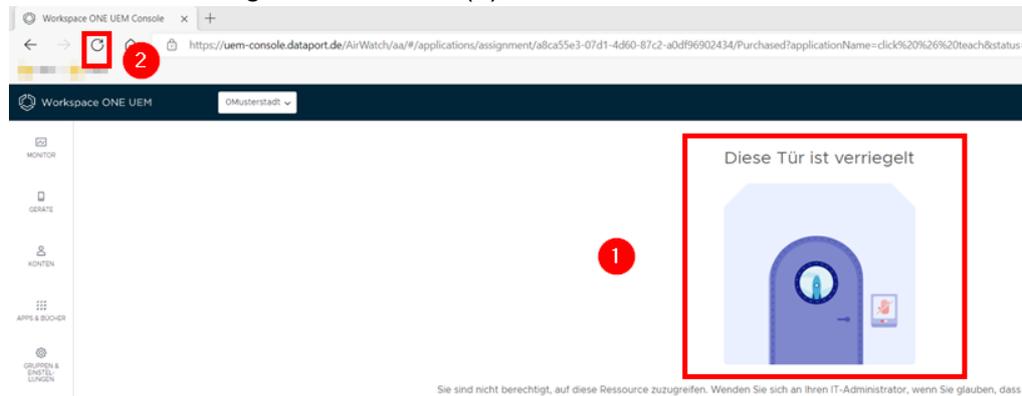
Zur App-Installation die passende Organisationseinheit (z. B. Schulträger) wählen (1), unter „Apps & Bücher“ (2) - „Anwendungen“ - „Systemeigen“ (3) und den Reiter „Gekauft“ (4) wählen, die gewünschte App markieren (5) und „Weitere Aktionen“ (6) sowie „Gerätezuweisung aktivieren“ (7) wählen:



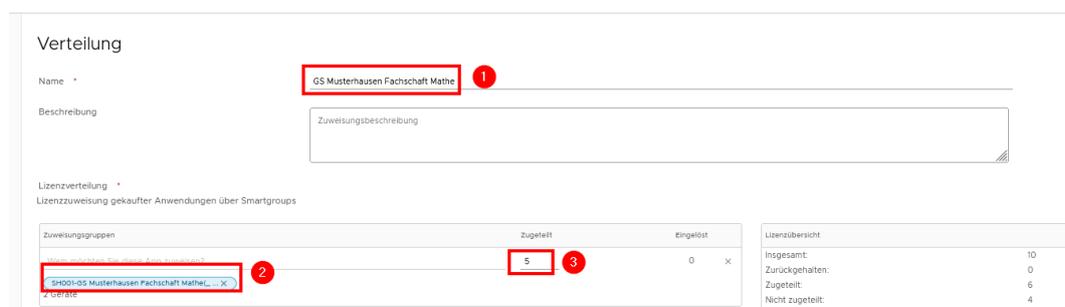
App markieren und „Zuweisen“ wählen:



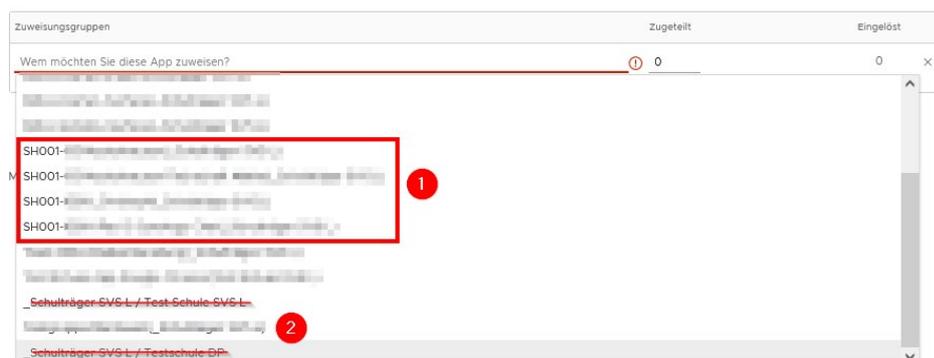
Hinweis: Wenn die Fehlermeldung „Diese Tür ist verriegelt“ (1) auftaucht, muss die Browserseite neu geladen werden (2):



Zuweisungsname (Name der Gruppe, die die App erhalten soll) eingeben (1) und Zuweisungsgruppe (2) mit Anzahl der benötigten Lizenzen (3) wählen:



Als Zuweisungsgruppe sollte nach Möglichkeit immer eine Zuweisungsgruppe (1) und keine Organisationsgruppe (2) gewählt werden, da man bei Organisationsgruppen keine Möglichkeit hat, die Eigenschaften der Gruppe (z. B. die Mitglieder) zu verändern:



Auswahl für „Methode zur Bereitstellung von Apps“ treffen. Dabei bedeutet „Automatisch“, dass die App direkt auf den Endgeräten der Zielgruppe installiert wird und „Bei Bedarf“, dass die App im Hub bereitgestellt wird und durch die jeweilige Lehrkraft selbst bei Bedarf installiert werden kann:

Verteilung

Name **GS-Musterhausen Fachschaft Mathe**

Beschreibung
 Zuweisungsbeschreibung

Lizenzverteilung **Lizenzzuweisung gekaufter Anwendungen über Smartgroups**

Zuweisungsgruppen	Zugeteilt	Eingelöst
Wem möchten Sie diese App zuweisen?	5	0
SH001-GS-Musterhausen Fachschaft Mathe (2 Geräte)		

HINZUFÜGEN

Methode zur Bereitstellung von Apps **Automatisch** Bei Bedarf

Lizenzübersicht	
Insgesamt:	10
Zurückgehalten:	0
Zugeteilt:	6
Nicht zugeteilt:	4
Eingelöst:	1

Zusätzlich unter dem Menüpunkt „Restriktionen“ (1) im linken Menü bei Bedarf folgende Punkte aktivieren (2):

Restriktionen (1)

Von EMM verwalteter Zugriff

Über den von EMM verwalteten Zugriff wird definiert, welche Geräte diese App von Intelligent Hub installieren können.

Wenn diese Einstellung deaktiviert ist, kann diese App von allen registrierten Geräten installiert werden.

Wenn diese Einstellung aktiviert ist:

- Nur von EMM verwaltete Geräte können diese App installieren.
- Wenn diese App durch Workspace ONE SDC, Version 20.10 oder höher, geschützt wird, wird der Zugriff blockiert, es sei denn, die App wird von EMM verwaltet, um sicherzustellen, dass diese App verwaltet wird, aktivieren Sie auf der Registerkarte „Restriktionen“ die Einstellung „App von MDM verwalten lassen, wenn der Benutzer es installiert hat“.

Bei Aufhebung der Registrierung entfernen 

Entfernen verhindern 

Sicherung der Anwendung verhindern 

App bei Benutzerinstallation unter MDM-Verwaltung stellen 

(2)

Hinweis: Wird das Häkchen für „Entfernen verhindern“ gesetzt, kann die App nicht durch den Benutzer bzw. die Benutzerin selbst vom Gerät deinstalliert werden, sondern nur über das UEM.

Im Anschluss die Zuweisung mit „Erstellen“, „Speichern“ und „Veröffentlichen“ anlegen.

Bis zu 5 Minuten warten und dann bei Bedarf prüfen, ob die Installation erfolgreich durchgeführt wurde:

- Dazu in der Appliste die betreffende App anhaken (1) und im Menü „Geräte verwalten“ (2) wählen:

Intern Öffentlich **Gekauft**

Filter **BESTELLUNG HINZUFÜGEN** **ANLAGEN SYNCHR**

ZUWEISEN **GERÄTE VERWALTEN** **APP AKTUALISIEREN**

Symbol	Name
<input checked="" type="checkbox"/> 	FreeOTP Authenticator 0Musterstadt ★★★★☆

(1) (2)

- Es erscheint nun eine Liste der Geräte, denen die App zugewiesen wurde:

Geräte verwalten - FreeOTP Authenticator

Installieren Entfernen Benachrichtigen Erneut einladen

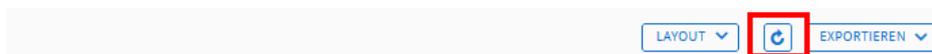
<input type="checkbox"/> Status	Letzte Aktion	Installationsstatus	VPP-Einladungsstatus
<input checked="" type="checkbox"/> Installiert	Installationsbefehl abgese...	Verwaltet	Nicht zutreffend

Elemente 1-1 von 1

Hinweis: Es kann sein, dass eine gerade installierte App noch als "nicht installiert" in den Gerätedetails auftaucht (Meldung: „Veraltet, zugewiesen, aber nicht installiert“). Diese Meldung sollte jedoch nach einiger Zeit verschwinden.

Wenn die App später automatische Updates erhalten soll, muss diese Funktion noch aktiviert werden:

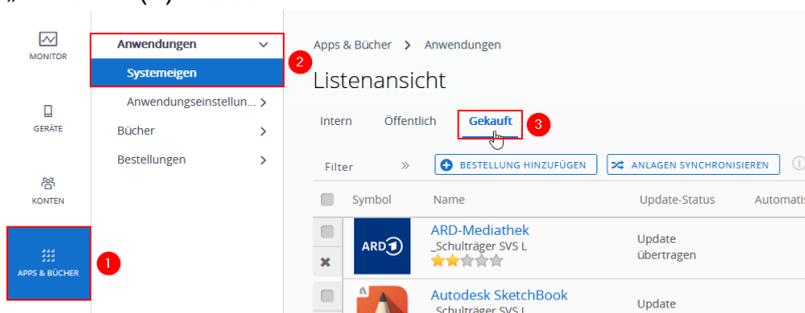
- Dazu unter „Apps & Bücher“ - „Anwendungen“ - „Systemeigen“ - Reiter „Gekauft“ die App markieren und im Anschluss "Weitere Aktionen" - „Automatische Updates aktivieren“ wählen.
- **Hinweis:** Falls die Option „Automatische Updates aktivieren“ nicht unter „Weitere Aktionen“ auftaucht, sollte die Seite über den Aktualisierungs-Button erneut geladen werden:



9.3 App-Deinstallation

Um eine App **nur von bestimmten Geräten** zu entfernen, sind folgende Schritte notwendig:

- Unter „Apps & Bücher“ (1) - „Anwendungen“ - „Systemeigen“ (2) und den Reiter „Gekauft“ (3) wählen:



- Dort die betreffende App markieren (1) und „Geräte verwalten“ (2) wählen:

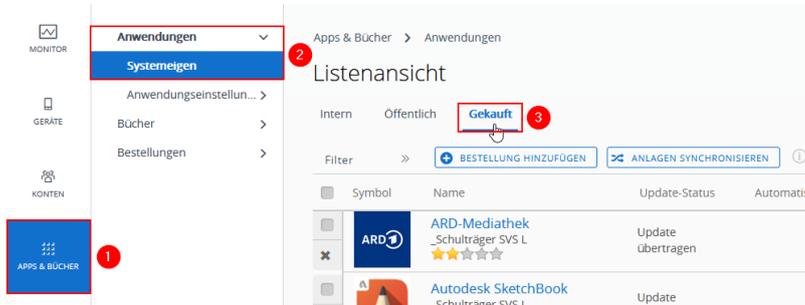


- Anschließend das betreffende Gerät markieren (1) und „Entfernen – Von ausgewählten Geräten entfernen“ (2) wählen:

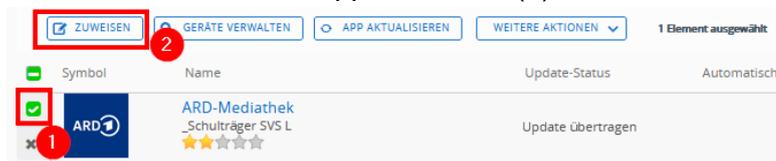


Um eine App von Geräten einer Zuweisungsgruppe zu entfernen, muss die Zuweisung gelöscht werden:

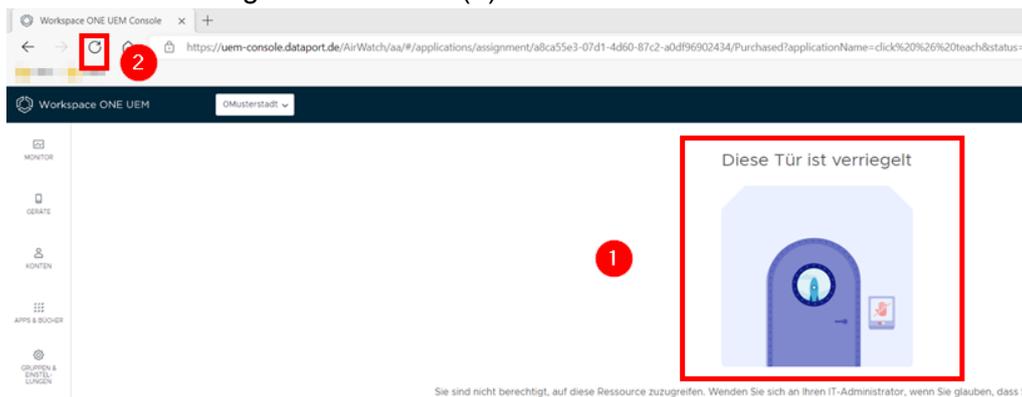
- Unter „Apps & Bücher“ (1) - „Anwendungen“ - „Systemeigen“ (2) und den Reiter „Gekauft“ (3) wählen:



- Dort die zu betreffende App markieren (1) und „Zuweisen“ (2) wählen:



Hinweis: Wenn die Fehlermeldung „Diese Tür ist verriegelt“ (1) auftaucht, muss die Browserseite neu geladen werden (2):



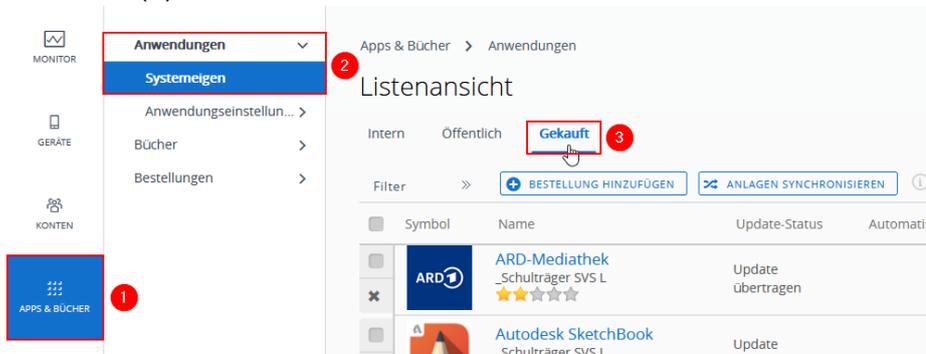
- Anschließend im Dreipunktmenü der betreffenden Zuweisung „Löschen“ wählen:
 ARD-Mediathek - Zuweisung



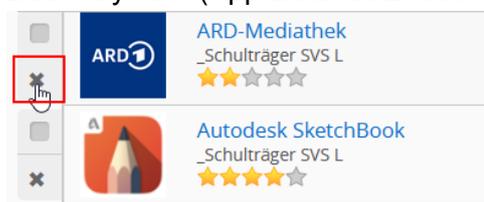
- Mit „Speichern“ und „Veröffentlichen“ bestätigen.

Um eine App **von allen zugewiesenen Geräten** zu entfernen, sind folgende Schritte notwendig:

- Unter „Apps & Bücher“ (1) - „Anwendungen“ - „Systemeigen“ (2) und den Reiter „Gekauft“ (3) wählen:

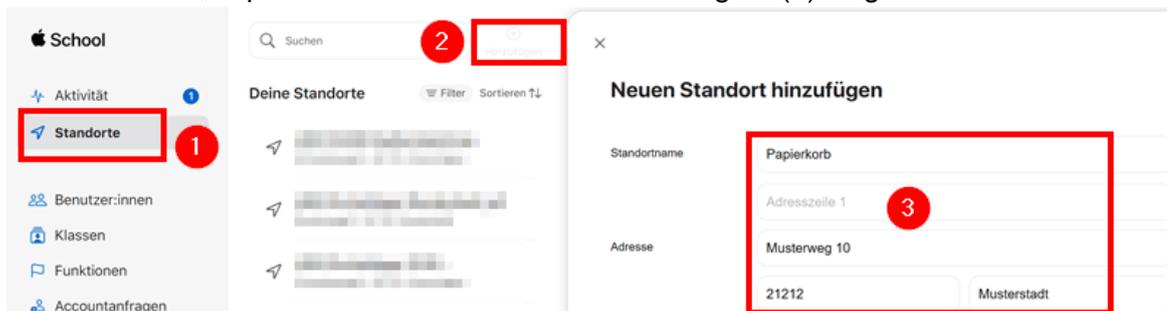
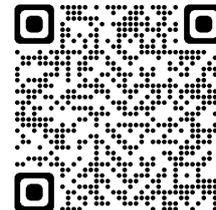


- Das x-Symbol (App-Datensatz löschen) vor der jeweiligen App wählen:

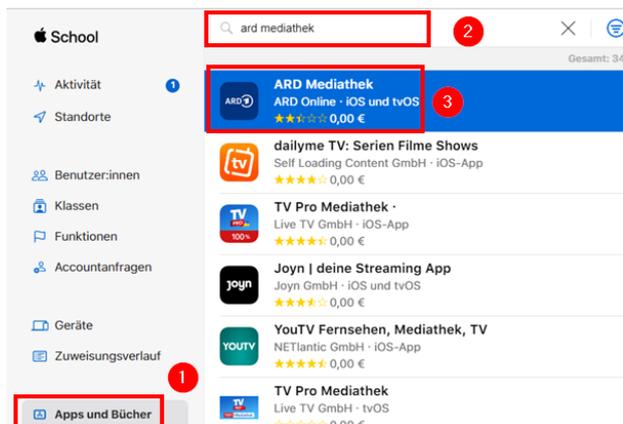


Die App verschwindet bis zur nächsten Synchronisierung mit dem Apple School Manager aus der Appliste im UEM. Um die App dauerhaft aus der Appliste im UEM zu entfernen, muss im Apple-School-Manager die Zuweisung der App zum UEM entfernt werden. Dazu sind nachfolgende Schritte notwendig:

- Zunächst in den Apple School Manager über <https://school.apple.com> einloggen.
- Wenn noch nicht vorhanden: einen Standort „Papierkorb“ anlegen. Dazu im Menü „Standorte“ (1) - „Hinzufügen“ (2) wählen, Standortname „Papierkorb“ und Anschrift des Schulträgers (3) eingeben:



- Mit „Sichern“ bestätigen.
- Unter „Apps und Bücher“ (1) die zu löschende App suchen (2) und die App auswählen (3):



- In den Appdetails unter „Lizenzen verwalten“ (1) den UEM-Standort auswählen (2) und unter „Übertragen“ (3) alle vorhandenen Lizenzen (4) für den Papierkorb (5) eintragen und übertragen (6):

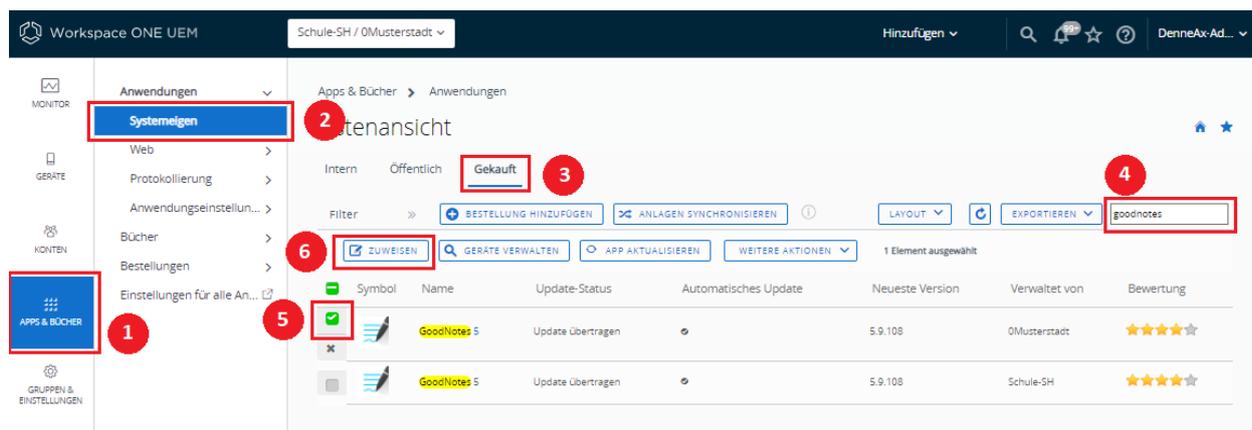


Hinweis: Es können nur Lizenzen in den Papierkorb verschoben werden, die keinem Gerät mehr zugeordnet sind. Ggf. muss hier zunächst die Synchronisierung zwischen UEM und ASM abgewartet werden. Nach erfolgreichem Verschieben in den Papierkorb und Synchronisierung mit dem ASM taucht die App auch nicht mehr im UEM auf.

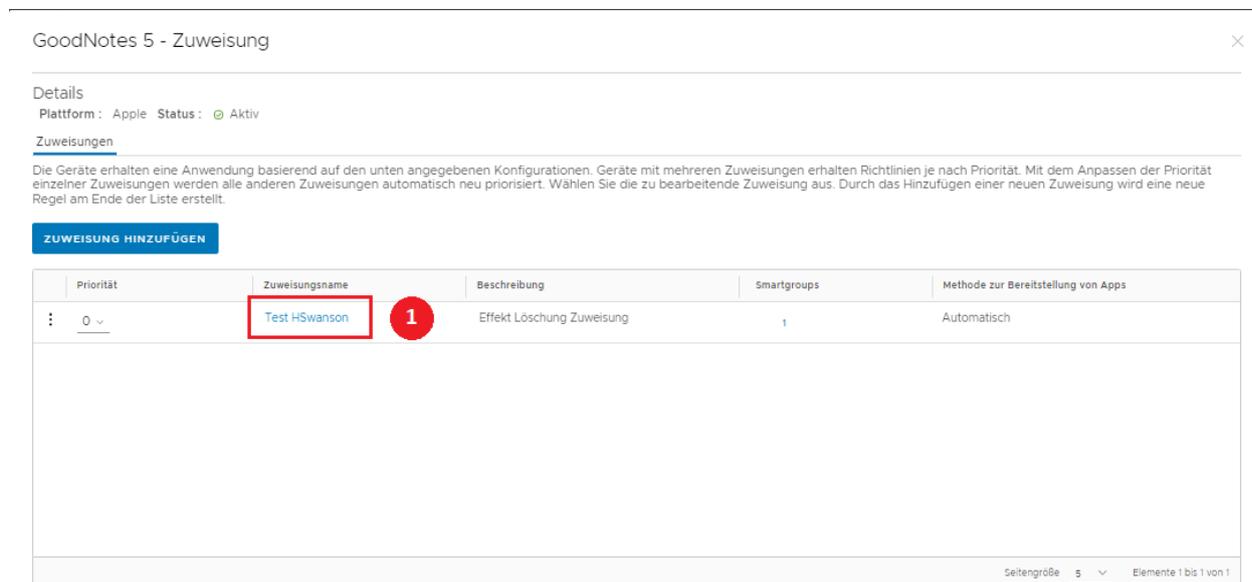
9.4 App-Konfiguration verteilen

Anwendungsspezifische Parameter, wie die Lizenzschlüssel einer App, lassen sich über das UEM als Parameter einer Zuweisung auf die ausgewählten iPads übertragen.

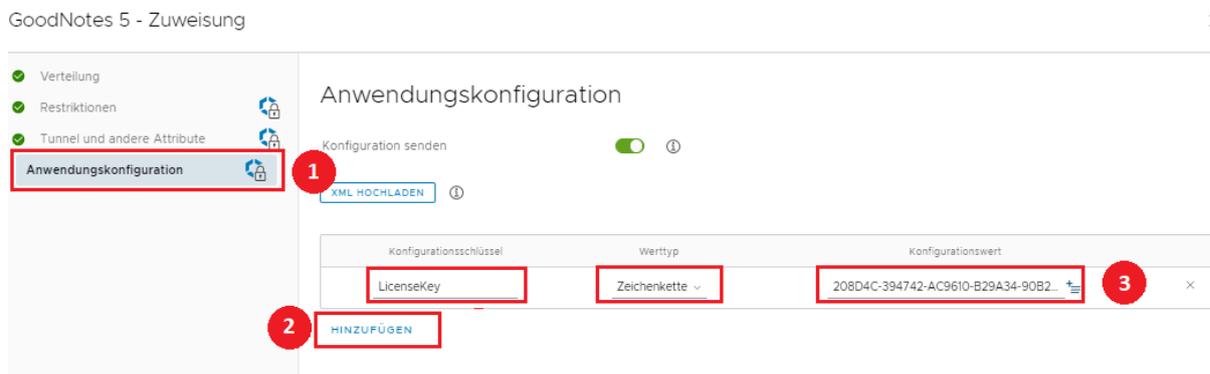
Dazu wählen Sie den Bereich „APPS & BÜCHER (1) und dort unter „Systemeigen“ (2) die „Gekauft“en Apps (3). Aufgrund der Anzahl verwalteter Apps empfiehlt es sich, die Anzahl der angezeigten Apps durch Eingabe eines Suchbegriffs im Suchfeld (4) zu reduzieren. Durch Aktivierung der Checkbox der App (5), werden im Funktionsmenü oberhalb der Listenansicht weitere Schaltflächen eingeblendet. Über die Schaltfläche „ZUWEISEN“ (6) öffnet sich ein Fenster mit allen aktiven Zuweisungen dieser App.



Ein Klick auf den Zuweisungsnamen (1) öffnet die Konfigurationsmaske der Zuweisung.



In der Konfigurationsmaske der Zuweisung im linken Auswahlménü auf die Funktion „Anwendungskonfiguration“ (1) wechseln und über „HINZUFÜGEN“ (2) den Eingabemodus aktivieren. Soll ein Lizenzschlüssel verteilt werden, ist der vom Anbieter der App bereitgestellte Namen des Lizenzschlüssels als „Konfigurationsschlüssel“ und der Lizenzschlüssel als „Konfigurationswert“ einzugeben (3). Den Abschluss der Eingabe anschließend durch speichern bestätigen.



Hinweis: Bitte unbedingt den Namen des Lizenzschlüssels wie vom Anbieter bereitgestellt übernehmen.

9.4.1 XML Import

Sollen mehrere Parameter als Konfigurationsschlüssel angelegt werden, so empfiehlt sich der Import über eine vorbereitete XML-Datei. Folgendes Beispiel wäre geeignet, um den Lizenzschlüssel für GoodNotes und das Upgrade-Flag für Version 6 anzulegen:

```
<managedAppConfiguration>
  <version>1</version>
  <bundleId>com.goodnotesapp.x </bundleId>
  <dict>
    <string keyName="LicenseKey">
      <defaultValue>
        <value>AAAAAA-BBBBBB-CCCCCC-DDDDDD-123456-V3</value>
      </defaultValue>
    </string>
    <boolean keyName="Goodnotes6Upgrade">
      <defaultValue>
        <value>>true</value>
      </defaultValue>
    </boolean>
  </dict>
</managedAppConfiguration>
```

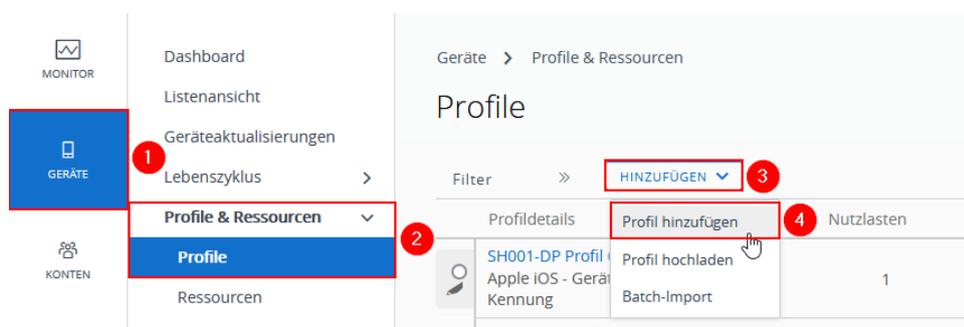
10 iPadOS: Profil erstellen

Hinweis: Mit dem im Juni 2024 durchgeführten Update des Workspace One UEM wurden Masken und Ablauf bei der Erstellung von Profilen für das iPad geändert. Die Zuweisung des Profils erfolgt beispielsweise erst nach Abschluss der Konfiguration, und folgt somit eher dem Prozess, wie man ihn von der Paketierung der internen Apps kennt.

Empfehlung: Um später mögliche Fehlerquellen besser identifizieren zu können, sollte man Profile nicht zu umfangreich gestalten und möglichst auf einen Aspekt (z. B. WLAN-Einstellungen, Webclips usw.) reduzieren.

Ein Profil wird über folgende Schritte erstellt:

Im Menü „Geräte“ (1) - „Profile & Ressourcen“ - „Profile“ (2) - „Hinzufügen“ (3) - „Profil hinzufügen“ (4) wählen:



Als Plattform „Apple iOS“ wählen:



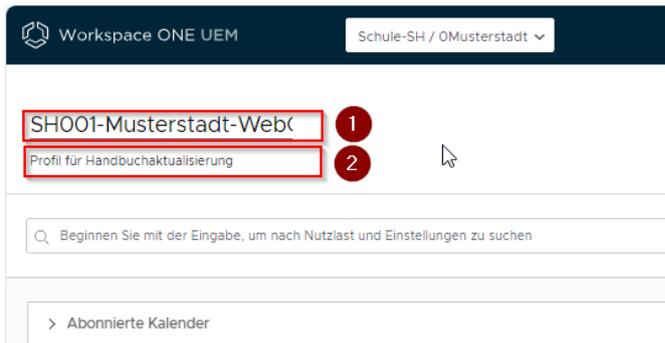
„Geräteprofil“ wählen:

Kontext wählen



In der Konfigurationsmaske ist ein Profilname (1) zu vergeben und kann eine Beschreibung (2) hinterlegt werden:

- Profilnamen sollte dem präferierten Schema folgen: GroupID (SH001), Bindestrich, Schulname, Profiltyp (z. B. SH001-GS Musterhausen Webclips).
Hinweis: Das Anzeigefeld ist auf 22 Zeichen beschränkt, der Name wird aber nicht abgeschnitten.
- Beschreibung sollte bei späteren Anpassungen und für den Support nützliche Hinweise liefern.



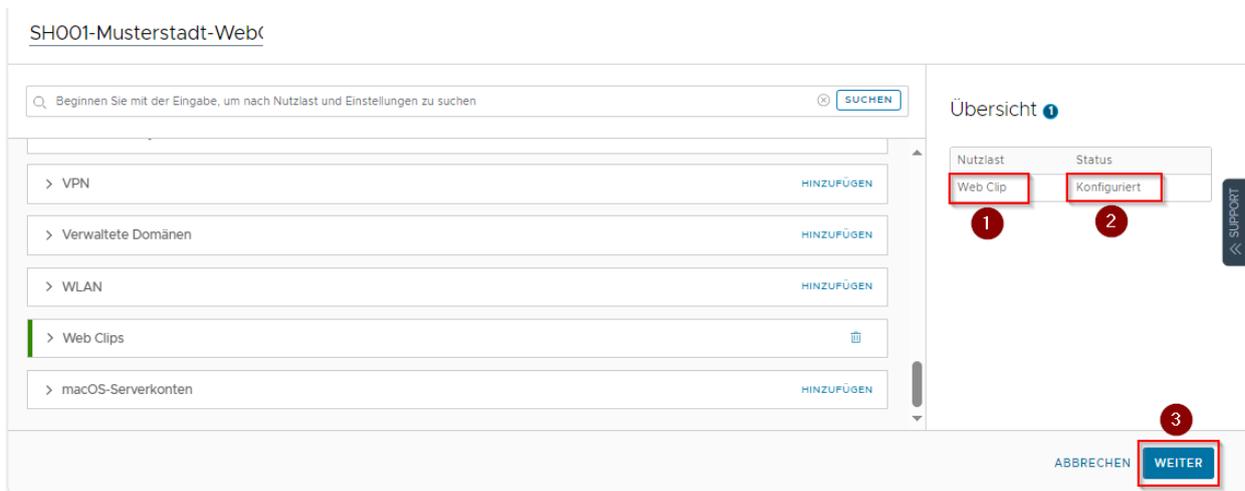
Anschließend zum gewünschten Profiltyp scrollen und Eingabemaske über den Dropdown-Pfeil (1) öffnen. HINZUFÜGEN (2) aktiviert die Eingabefelder.



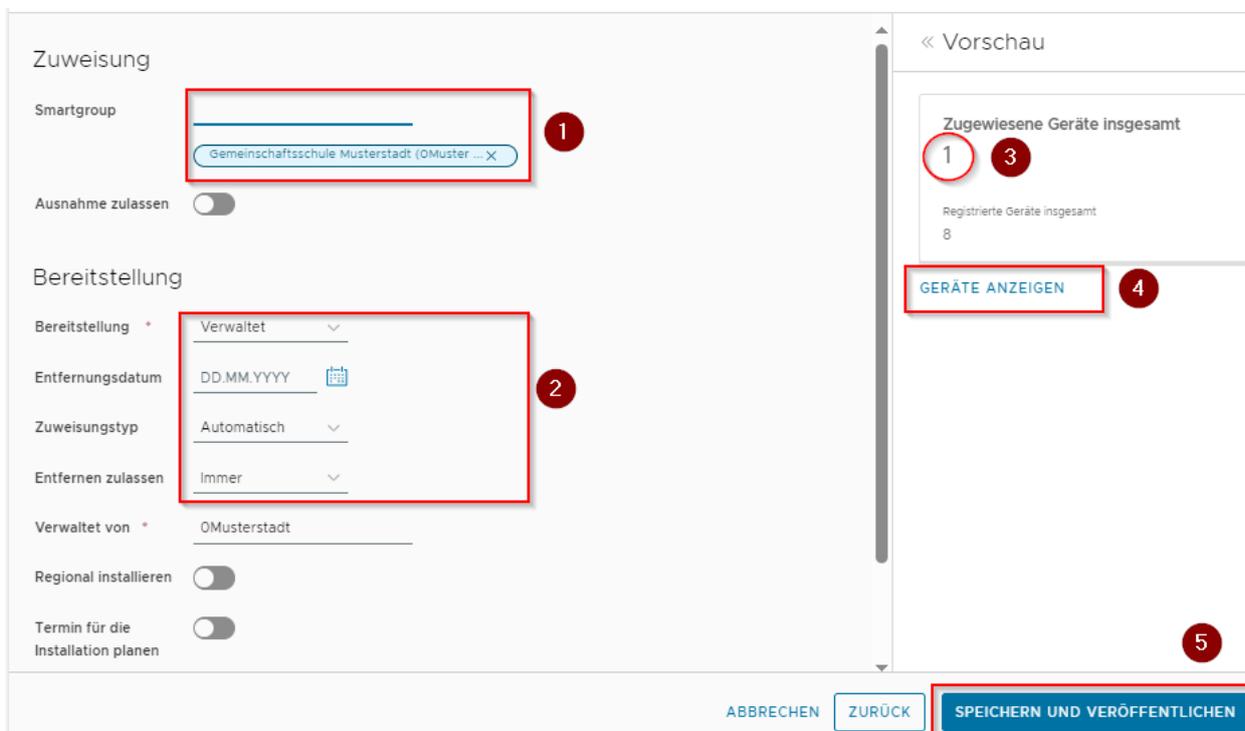
Für den WebClip müssen eine Beschriftung (1) und die URL (2) konfiguriert werden. Über den Papierkorb (3) lassen sich zu Testzwecken erstellte oder nicht mehr benötigte Elemente entfernen. Der Upload eines Symbols ist empfehlenswert.



HINZUFÜGEN erzeugt jeweils einen Eintrag in der Tabelle im Bereich „Übersicht“ (1). Ist die Konfiguration abgeschlossen wechselt der Status von „Nicht konfiguriert“ auf „Konfiguriert“ (2). WEITER (3) schließt die Konfiguration des Profils ab und führt zur Zuweisung.



Unter Smartgroup (1) ist mindestens eine Zuweisungsgruppe anzugeben. Die Bereitstellungsparameter (2) können je nach Bedarf angepasst werden. Zugewiesene Geräte (3) sind alle iPads in der/den gewählten Zuweisungsgruppe/n. GERÄTE ANZEIGEN (4) listet alle iPads der Zuweisung tabellarisch auf. Mit SPEICHERN UND VERÖFFENTLICHEN (5) wird die Zuweisung abgeschlossen.

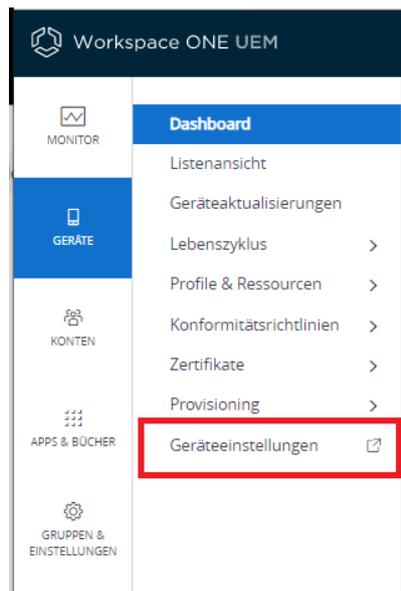


11 iPadOS: Schriftarten hinzufügen

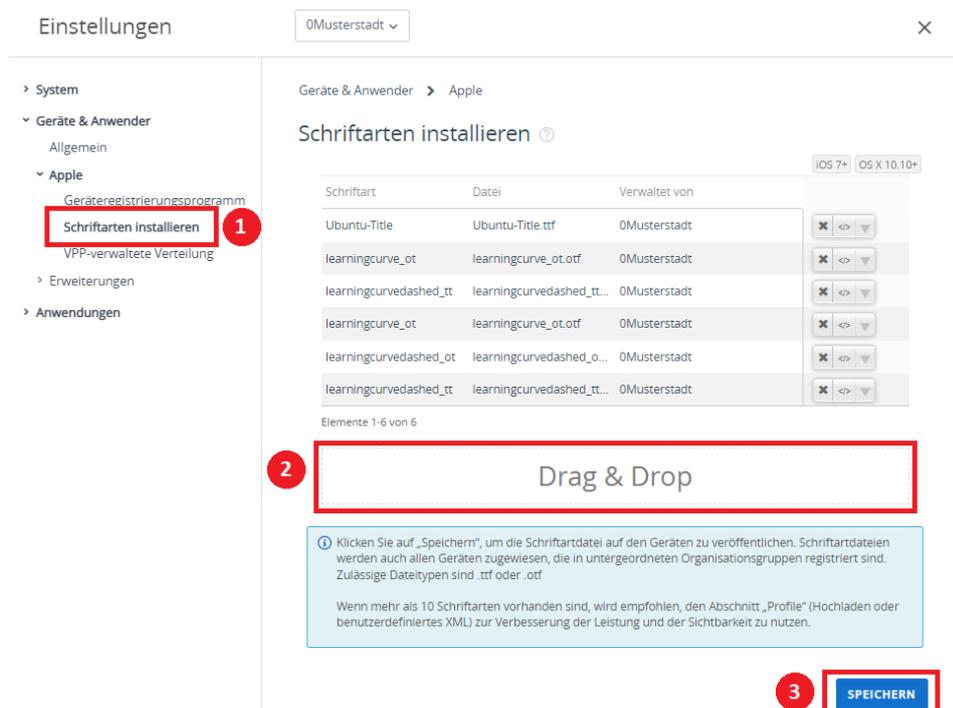
Das UEM erlaubt die Installation zusätzlicher Schriftarten auf den verwalteten iPads. Die Schriftarten müssen dabei nicht über den Apple Schoolmanager erworben und - bei der hier beschriebenen Vorgehensweise - den Geräten nicht speziell zugewiesen werden.

Hinweis: Das UEM erlaubt keine Prüfung kostenpflichtiger Lizenzen. Verwenden Sie ausschließlich kostenfreie Fonts oder Fonts, für die ausreichend Lizenzen erworben wurden!

Zur Anlage wechseln Sie in der Rubrik Geräte in die Geräteeinstellungen:



Wählen Sie anschließend im Bereich „Apple“ die Funktion „Schriftart installieren“ (1)



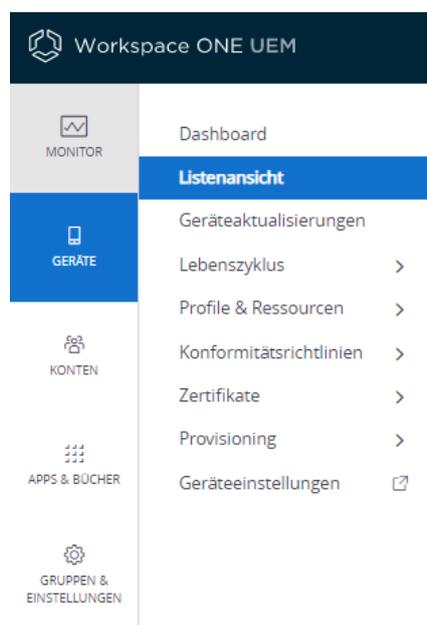
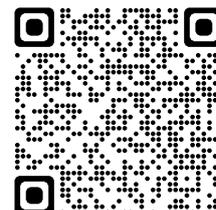
Ziehen Sie den oder die gewünschten Font-Dateien mit der Maus in das Feld „Drag & Drop“ (2). Durch „Speichern“ (3) werden die Fonts auf allen dem Schulträger zugewiesenen iPads installiert.

Hinweis: Unterstützt werden Dateien vom Typ *.ttf und *.otf. Die Extension **muss** klein geschrieben werden. Andernfalls wird die Datei als ungültiges Format zurückgewiesen.

Hinweis: Fonts lassen sich bei Bedarf auf gleichen Wege von den verwalteten iPads entfernen.

12 iPadOS: Kennung zurücksetzen

Das Zurücksetzen des Gerätepasswortes kann durch dezentrale Administratoren und Administratorinnen (Schulträger, Dienstleister, RBZ/BBS) oder Dataport erfolgen. Das folgende Kapitel beschreibt die Vorgehensweise für die dezentralen Administratoren und Administratorinnen. Soll das Zurücksetzen über Dataport erfolgen, so ist durch die betroffene Lehrkraft oder die Schulleitung ein Ticket über das Helpdesk-Formular unter <https://www.secure-lernetz.de/helpdesk> im Bereich „LK-Endgeräte“ – „Support“ zu eröffnen.



Nach der Anmeldung beim UEM-wählen Sie die Listenansicht im Bereich „Geräte“:

Wählen Sie das zu entsperrende Gerät. Sind sehr viele Geräte für Ihre Schule/Ihren Schulträger registriert, empfiehlt sich die Verwendung der Suchfunktion (Liste durchsuchen). Hier kann sowohl über die Geräte-ID als auch über den Namen der Lehrkraft gesucht werden.

Klicken Sie auf die Geräte-ID um in die Detailansicht des Gerätes zu wechseln.





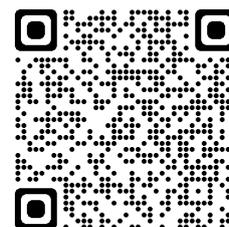
Öffnen Sie am rechten Fensterrand das Menü „WEITERE AKTIONEN“ und wählen Sie die Funktion „Kennung löschen“- „Gerät“.
 Bestätigen Sie die nachfolgende Abfrage, um die Funktion zu aktivieren.

Die Lehrkraft wird nun am iPad aufgefordert innerhalb der nächsten Stunde, einen neuen Geräte-Code zu vergeben.



13 iPads: Gerät zurücksetzen

Das Zurücksetzen der Kennung und des Gerätes erfolgt bei Bedarf ausschließlich über Dataport. Dazu muss ein Ticket über das Helpdesk-Formular unter <https://www.secure-lernetz.de/helpdesk> im Bereich „LK-Endgeräte“ – „Support“ aufgegeben werden.



14 Windows: Paket-Erstellung, -Installation und -Deinstallation

14.1 Paket-Erstellung

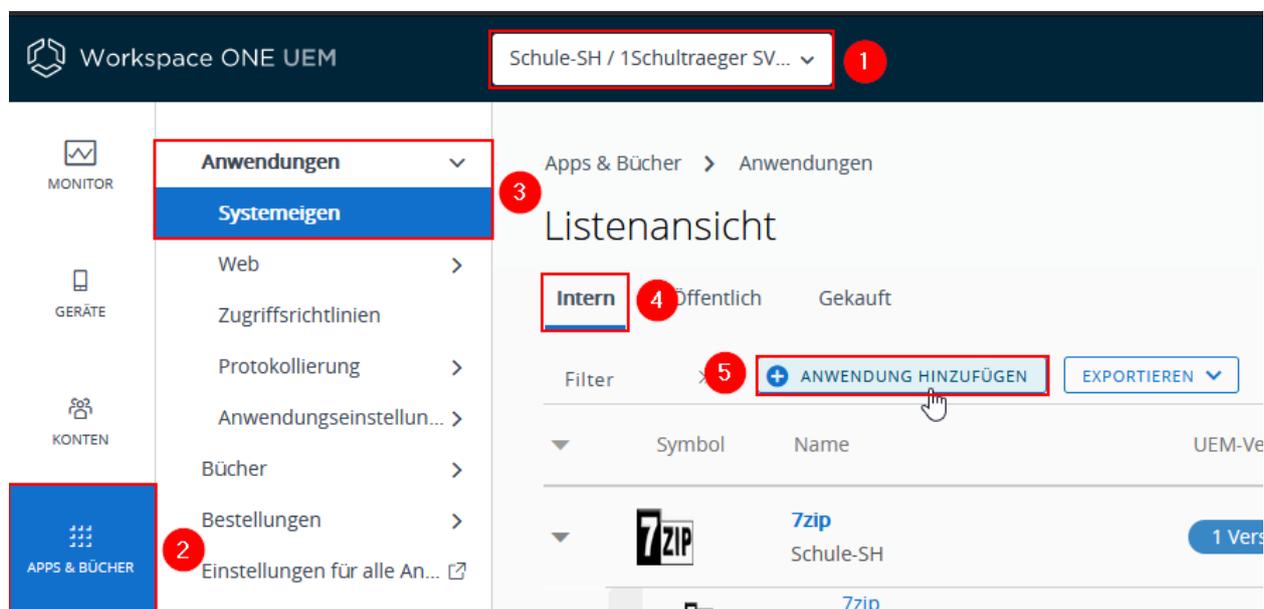
Bevor das Paket erstellt werden kann, muss zunächst die Installationsdatei (MSI- oder EXE-Datei) des Programms heruntergeladen werden.

Hinweis: Werden zusätzlich zur Installationsdatei weitere Dateien und Ordner benötigt (zum Beispiel der Inhalt einer Installations-CD/DVD), müssen die Installationsdatei und alle zugehörigen Dateien und Ordner in eine ZIP-Datei mittels 7Zip gepackt und hochgeladen werden.

Soll eine ISO-Datei verwendet werden, muss diese zunächst extrahiert werden und dann in einer ZIP-Datei zusammengefasst werden.

Auch ein mit dem „PowerShell App Deployment Toolkit“ (<https://psappdeploytoolkit.com/>) erstelltes Paket kann in Form einer ZIP-Datei hochgeladen werden. Die darin enthaltenen Installationsdateien und Skripte (zum Beispiel zum Verteilen einer Lizenz oder zum Ausführen von weiteren Aktionen) können dann über die Starterdatei „Deploy-Application.exe“ ausgeführt werden.

Anschließend zur Paketerstellung ins UEM wechseln, die passende Organisationseinheit (z. B. Schulträger) wählen (1), unter „Apps & Bücher“ (2) - „Anwendungen“ - „Systemeigen“ (3), den Reiter „Intern“ (4) wählen und auf „Anwendung hinzufügen“ klicken:



Anschließend erscheint ein Fenster, in dem die Felder schon vorausgefüllt sind. Das Feld zur Organisationsgruppen-ID (1) muss nicht geändert werden. Unter „Hochladen“ (2) kann die heruntergeladene Installationsdatei hochgeladen werden:

Anwendung hinzufügen

Organisationsgruppen-ID * **1**

App-Datei * **HOCHLADEN** **2**

Dazu auf „Durchsuchen...“ (1) klicken, welches ein weiteres Fenster öffnet. Dort kann die heruntergeladene Installationsdatei ausgewählt und mit „Öffnen“ bestätigt werden. Sobald die Datei ausgewählt wurde zeigt (2) eine Vorschau des Dateinamens an. Anschließend auf „Speichern“ (3) klicken:

Hinzufügen ×

Typ Lokale Datei Link

1 **2**

Sie haben 2737 MB von 20000 MB verwendet.

3

Darauf kann festgelegt werden, ob es eine „Abhängigkeits-App“ (1) für ein anderes Programm handelt. Manche älteren Programme benötigen bestimmte Bibliotheken oder Framework-Pakete, bspw. *Visual Studio C++ Redistributable*, welche von diesen nicht in der Installationsdatei enthalten sind und somit eigenständig verteilt werden müssen. Im Regelfall auf „Nein“ belassen und auf „Weiter“ (2) klicken:

Anwendung hinzufügen

Organisationsgruppen-ID *

App-Datei *

Ist dies eine Abhängigkeits-App? **1**

Anschließend darauf achten, dass „Details“ (1) aufgerufen ist. Hier den Namen des Paketes (2)

eintragen und gegebenenfalls die Prozessorarchitektur (3) von „32-bit“ auf „64-bit“ ändern:

Details 1 Dateien Bereitstellungsmöglichkeiten Bilder Nutzungsbedingungen

Name * 2 Nextcloud ⓘ

Verwaltet von 1Schultraeger SVS L

Anwendungs-ID * {FD2FCCA9-BB8F-4485-8F70-A0621B84A7F4}

App-Version * 3.3.4.20210920

Build-Version {83FFDFF0-CE7B-4684-9A78-AD07972A17DC}

Aktuelle UEM-Version 3 . 3 . 4 . 20210920 ⓘ

Unterstützte Prozessorarchitektur 3 32-bit ⓘ

Für die **EXE-Datei** müssen folgende Schritte zusätzlich unternommen werden. Auf „Bereitstellungsmöglichkeiten“ (1) wechseln, zu „Wie die Installation erfolgen soll“ (2) gehen und den „Installationsbefehl“ (3) für die EXE-Datei angeben. Dieser Befehl unterscheidet sich je nach Hersteller:

Details Dateien **Bereitstellungsmöglichkeiten** 1 Bilder Nutzungsbedingungen

Wie die Installation erfolgen soll 2

Installationskontext GERÄT BENUTZER ⓘ

Installationsbefehl * 3 Beispiel: setup.exe /config exampleconfig.xml ⓘ

Administratorenprivilegien JA NEIN ⓘ

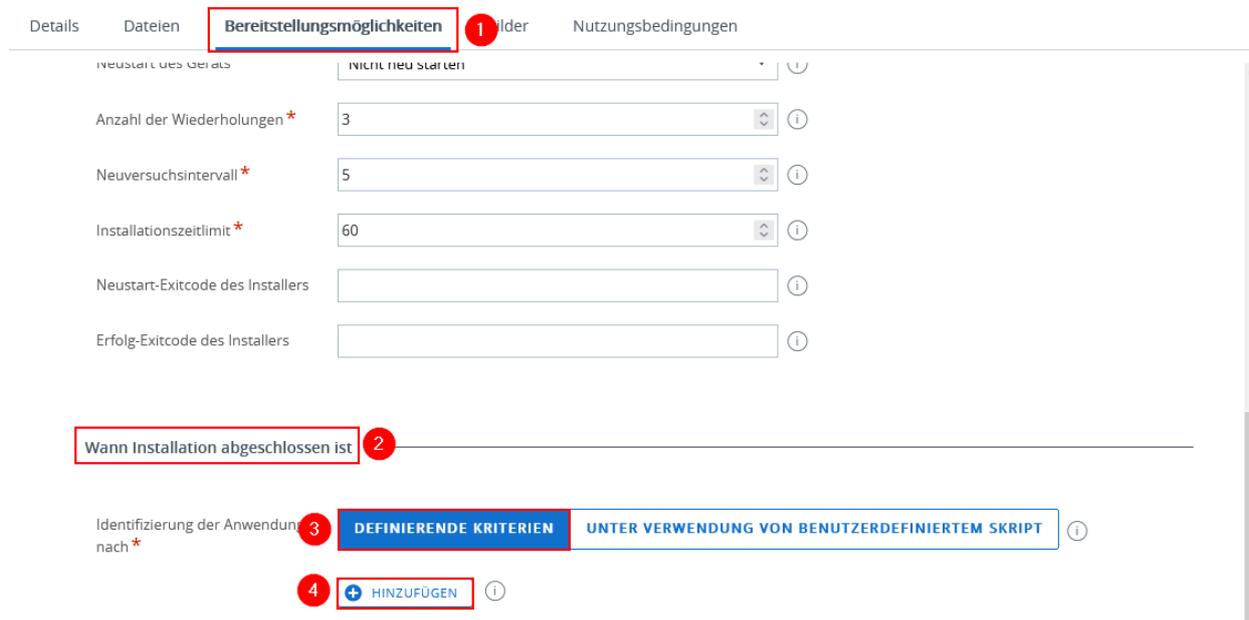
Neustart des Geräts Nicht neu starten ⓘ

Die folgende Tabelle stellt eine Übersicht von Beispielen zu verschiedenen Programmen dar:

Software	Installationsbefehl
Audacity	audacity-win-3.0.0.exe /VERYSILENT /NORESTART /LOG="%temp%\Audacity.log"
Shotcut	shotcut-win64-210321.exe /S
CamStudio	CamStudioSetup.exe /VERYSILENT
OpenBoard	OpenBoard_Installer_1.5.4.exe /VERYSILENT

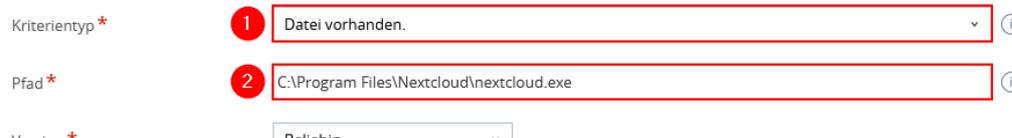
Ab hier gilt die Anleitung wieder für MSI- und EXE-Installationsdateien.

Im Reiter „Bereitstellungsmöglichkeiten“ (1) unter dem Bereich „Wann Installation abgeschlossen ist“ (2) unter „Definierende Kriterien“ (3) auf „Hinzufügen“ (4) klicken:



Im darauf erscheinenden Fenster den „Kriterientyp“ (1) auf „Datei vorhanden“ wechseln und den Zielpfad des installierten Paketes (2) angeben und mit „Speichern“ abschließen:

Kriterien hinzufügen

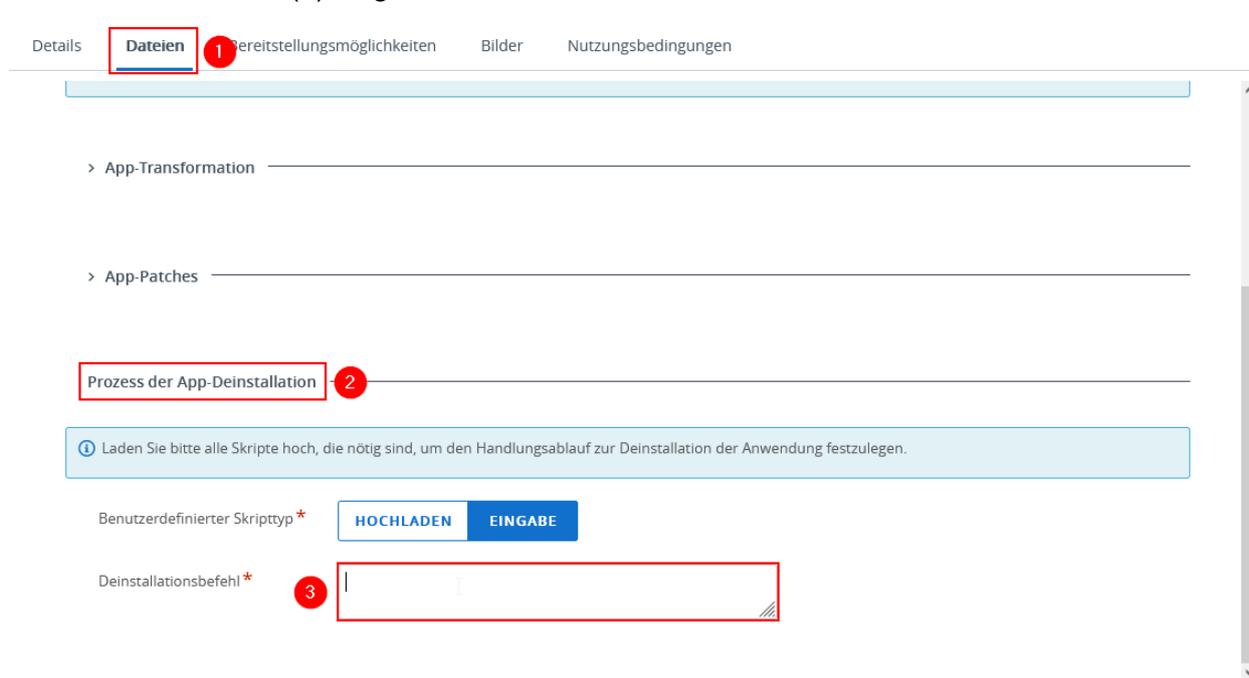


Beispiele für Kriterieneinstellungen finden Sie in der nachfolgenden Tabelle:

Software	Definierende Kriterien
Audacity	Datei vorhanden: C:\Program Files (x86)\Audacity\audacity.exe
Shotcut	Datei vorhanden: C:\Program Files\Shotcut\Shotcut.exe
CamStudio	Datei vorhanden: C:\Program Files\CamStudio 2.7\recorder.exe
OpenBoard	Datei vorhanden: C:\Program Files (x86)\OpenBoard\OpenBoard.exe

Für die **EXE-Datei** müssen weitere Schritte unternommen werden:

Dazu auf „Dateien“ (1) wechseln, in den Bereich „Prozess der App-Deinstallation“ (2) und den Deinstallationsbefehl (3) eingeben:

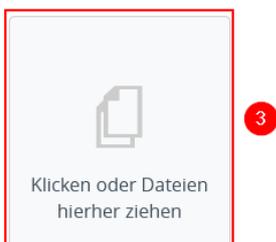


Diese Deinstallationsbefehle unterscheiden sich je nach Hersteller. Folgende Tabelle liefert Beispiele für einige Programme:

Software	Deinstallationsbefehl
Audacity	C:\Program Files (x86)\Audacity\unins000.exe /VERYSILENT /NORESTART
Shotcut	C:\Program Files\Shotcut\uninstall.exe /S
CamStudio	C:\Program Files\CamStudio\uninstall.exe /S
OpenBoard	C:\Program Files (x86)\unins000.exe /VERYSILENT

Ab hier an gilt die Anleitung wieder für MSI- und EXE-Installationsdateien.

Im Reiter „Bilder“ (1) kann anschließend ein Bild für den Hub hochgeladen werden. Dazu „Symbol“ (2) auswählen und durch klicken von (3) die Datei auswählen:

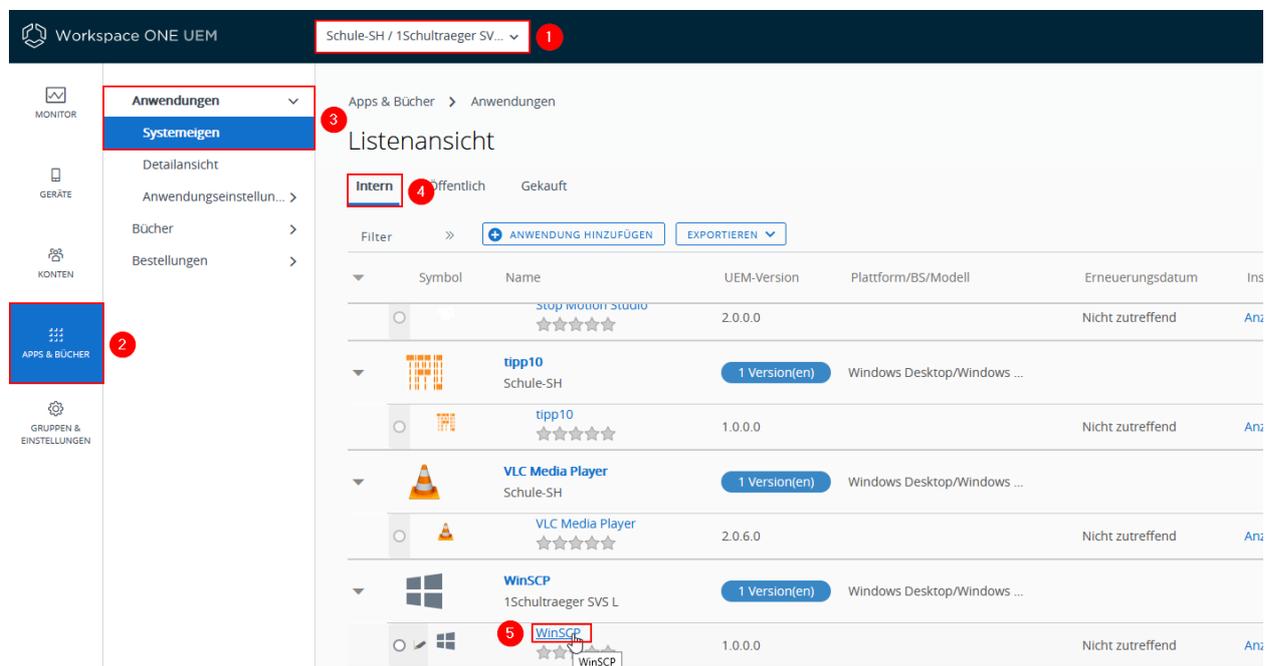


Zum abschließenden Speichern des Pakets auf „Speichern und Zuweisen“ klicken.

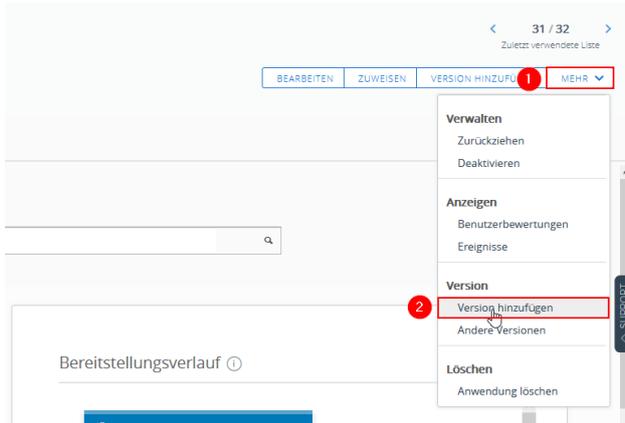
Die Schritte werden dazu im Kapitel [Paket-Installation](#) beschrieben.

14.2 Paket-Aktualisierung

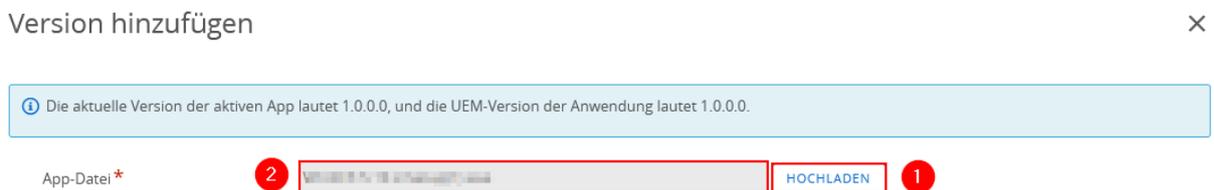
Um ein Paket zu aktualisieren, ins UEM wechseln, die passende Organisationseinheit (z. B. Schulträger) wählen (1), unter „Apps & Bücher“ (2) - „Anwendungen“ - „Systemeigen“ (3) und den Reiter „Intern“ (4) wählen und in der Spalte „Name“ unter dem jeweiligen Anwendungsnamen auf den Namen der zuletzt angelegten Version (5) klicken:



Auf der folgenden Seite auf „Mehr“ (1) und anschließend auf „Version hinzufügen“ (2) klicken:



Daraufhin die neue Version der Installationsdatei des Pakets mittels „Hochladen“ (1) hochladen. Eine Vorschau des Dateinamens befindet sich unter (2):

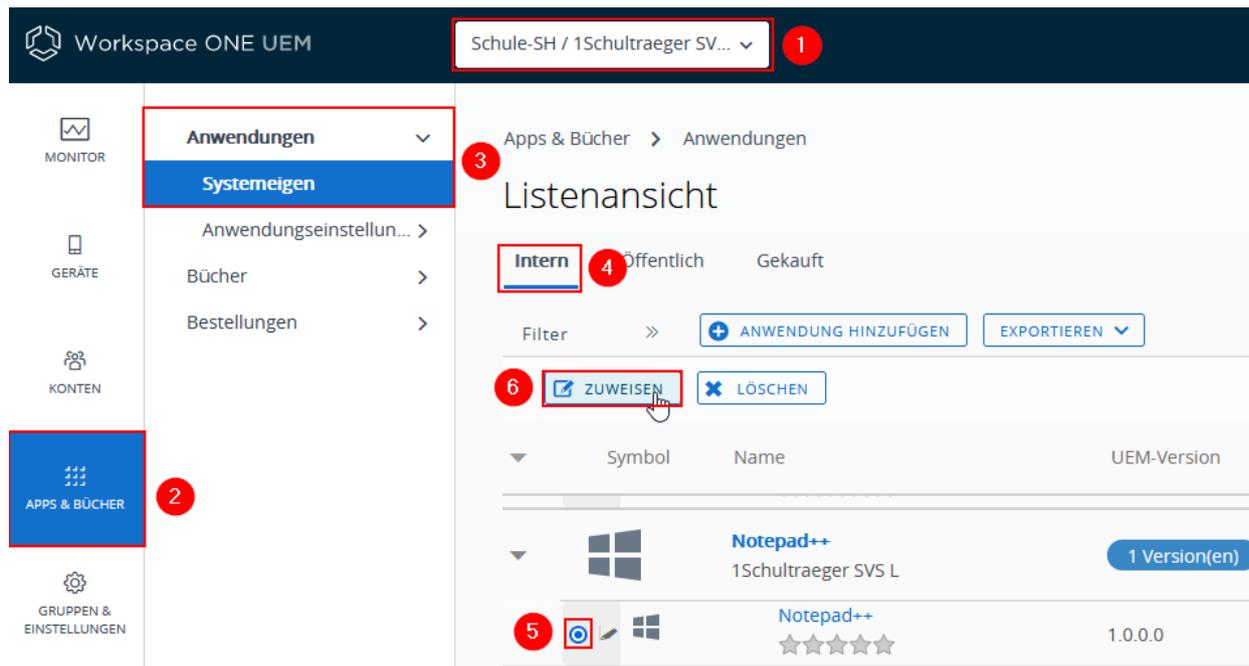


Mit „Speichern“ abschließen.

Die darauffolgenden Schritte laufen wie im Kapitel [Paket-Erstellung](#) ab.

14.3 Paket-Installation

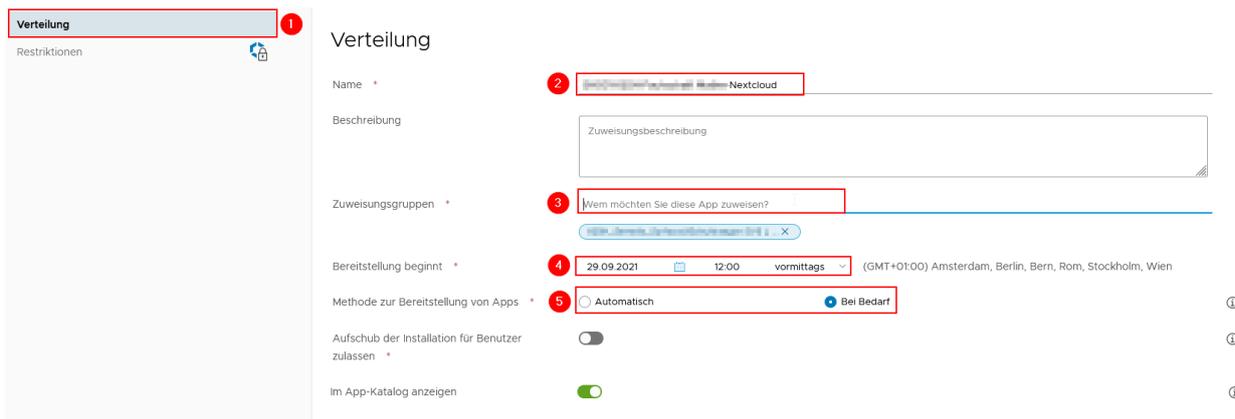
Um ein Paket installieren zu können, muss im UEM die passende Organisationseinheit (z. B. Schulträger) gewählt werden (1), unter „Apps & Bücher“ (2) - „Anwendungen“ - „Systemeigen“ (3) und den Reiter „Intern“ (4) wählen. Anschließend von dem Programm auf die jeweilige Version auswählen (5) und auf „Zuweisen“ (6) klicken:



Hinweis: Wenn die Fehlermeldung „Diese Tür ist verriegelt“ (1) auftaucht, muss die Browserseite neu geladen werden (2):



Daraufhin im folgenden Fenster auf „Zuweisung hinzufügen“. Dann kann die Zuweisung des das Pakets eingestellt werden. Dazu auf „Verteilung“ (1) klicken. Dann den Zuweisungsnamen (z. B. Name der Gruppe, die die App erhalten soll) eingeben (2) und Zuweisungsgruppe (3) wählen:



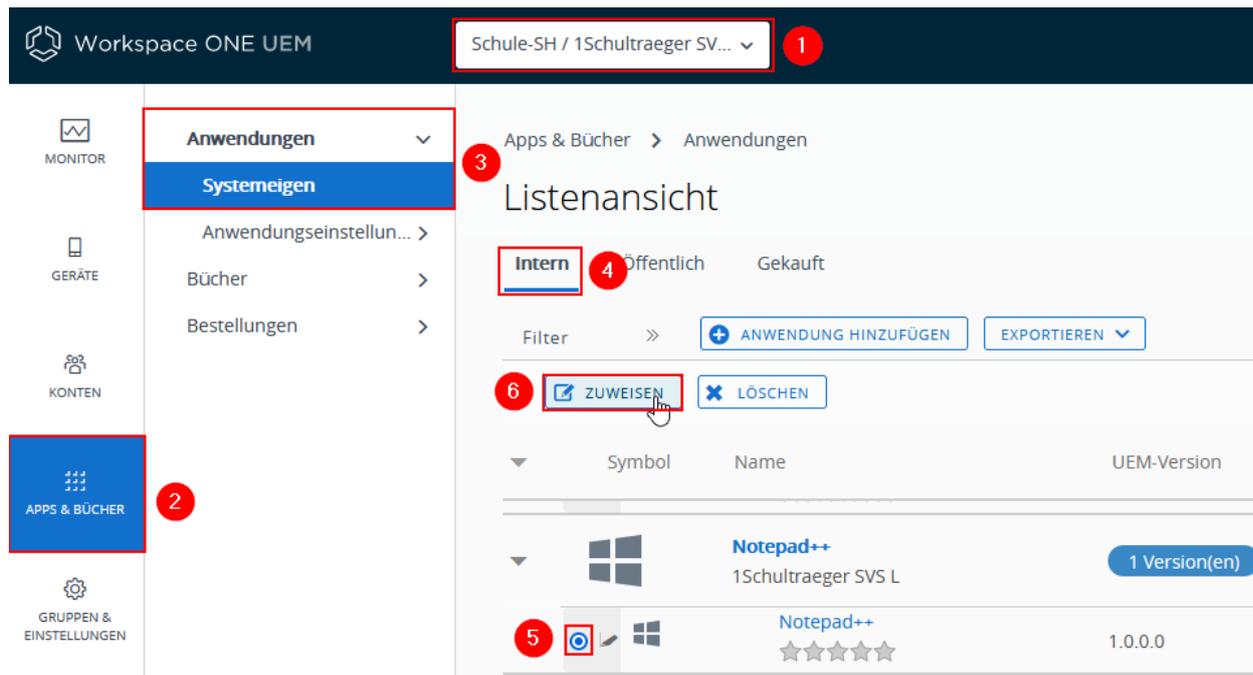
Als Zuweisungsgruppe sollte nach Möglichkeit immer eine Zuweisungsgruppe (1) und keine Organisationsgruppe gewählt werden, da man bei Organisationsgruppen keine Möglichkeit hat, die Eigenschaften der Gruppe (z. B. die Mitglieder) zu verändern:



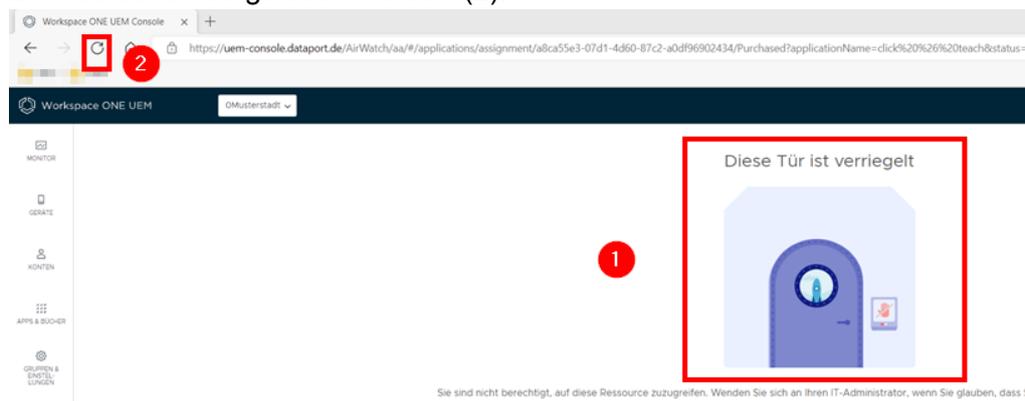
Daraufhin kann noch der Beginn Bereitstellung (4) eingestellt werden und ob diese „Automatisch“ oder „Bei Bedarf“ (5) im Hub bereitsteht. Abschließend auf durch „Erstellen“ und „Speichern“ klicken, um das Paket zuzuweisen.

14.4 Paket-Deinstallation

Um ein Paket deinstallieren zu können, muss im UEM die passende Organisationseinheit (z. B. Schulträger) gewählt werden (1), unter „Apps & Bücher“ (2) - „Anwendungen“ - „Systemeigen“ (3) und den Reiter „Intern“ (4) wählen. Anschließend von dem Programm auf die jeweilige Version auswählen (5) und auf „Zuweisen“ (6) klicken:



Hinweis: Wenn die Fehlermeldung „Diese Tür ist verriegelt“ (1) auftaucht, muss die Browserseite neu geladen werden (2):



Daraufhin bei der jeweiligen Zuweisung auf die drei Punkte (1) und löschen (2) klicken. Durch Klicken von „Speichern“ wird die Löschung der Zuweisung durchgeführt:



Hinweis: Wenn es für die zu löschende App aktive Zuweisung gibt, so werden die Zuweisung deaktiviert und die App bekommt den Status „retired“. Die App ist in der Listenansicht nicht mehr zu erkennen, aber weiterhin im System vorhanden. Die Zuweisungen sind weiterhin mit der Zuweisungsgruppe verknüpft. Inaktive Apps können über den Filter Status sichtbar gemacht werden.

14.5 Lizenzverteilung

Die Lizenzierung einer kostenpflichtigen Software kann über verschiedene Wege durchgeführt werden. Der Weg ist auch davon abhängig, wie der jeweilige Hersteller der Software die Lizenzierung vorgegeben hat.

- Wenn der Lizenzschlüssel im Installationsbefehl übergeben werden kann, so ist die direkte Verteilung über das Erstellen eines Paketes im UEM möglich (siehe Kapitel [Paket-Erstellung](#)).
- Bei einigen Anwendungen lässt sich eine separate Lizenzdatei oder eine Konfigurationsdatei in das Installations-Paket in Form einer ZIP-Datei integrieren (siehe Kapitel [Microsoft Office-Paketierung](#)). Ggf. muss dabei mit Hilfe einer Skriptdatei oder mit Hilfe des Powershell App Deployment Toolkits das Ausführen bzw. Bereitstellen der Datei während der Paketinstallation vorgenommen werden.
- Anstatt die Lizenzdatei direkt in das Paket zu integrieren, lässt sich diese auch vor oder nach der Paketinstallation an die Geräte verteilen. Dies ist zum Beispiel bei bereits vorhandenen lizenzpflichtigen Anwendungen im internen Appstore notwendig, die durch das Land bereitgestellt wurden. Wie das Kopieren der Lizenzdatei für ausgewählte Anwendungen funktioniert, wird im nachfolgenden Kapitel beschrieben (siehe Kapitel [Lizenzdatei kopieren](#)).
- Wenn die Freischaltung der Software nicht über das UEM geschehen kann, muss die Aktivierung manuell durch den Nutzer bzw. die Nutzerin am Endgerät vorgenommen werden.

14.5.1 Lizenzdatei kopieren

Wenn eine lizenzpflichtige Software ohne integrierte Lizenz im internen Appstore bereitgestellt wird, kann die Lizenzierung vor oder nach der Installation durch die Verteilung der jeweiligen Lizenzdatei vorgenommen werden. Eine manuelle Lizenzierung am Endgerät durch die jeweilige Lehrkraft ist dann nicht mehr notwendig. Im internen Appstore befinden sich bereits einige vom Land bereitgestellte Pakete, die eine Lizenzierung benötigen: z. B. Lernwerkstatt, Budenberg oder ActiveInspire.

Folgende Schritte sind zum Verteilen der Lizenzdatei notwendig:

- Lizenzdatei besorgen/erstellen/anpassen.
- Lizenzdatei über das UEM in den korrekten Zielpfad der Endgeräte kopieren (siehe Kapitel [Windows: Kopieren von Dateien/Ordnern](#)).

Informationen zu Lizenzdateien und zugehörigen Pfaden ausgewählter Anwendungen finden Sie in der nachfolgenden Tabelle:

Software	Dateiname, Hinweise	Zielpfad
ActiveInspire	<p>.inspire_license.xml</p> <p>Die Lizenzdatei findet man auf einem Gerät, auf dem ActiveInspire bereits mit der Lizenz aktiviert wurde, im Ordner C:\ProgramData\Promethean\ActivInspire. Alternativ lässt sich diese auch manuell mit dem nachfolgenden Inhalt erstellen:</p> <pre><License> <username/> <organization/> <serial>aaaabbbbccccddddeeee</serial> </License></pre> <p>Hinweis: Die Buchstabenkombination „aaaabbbbccccddddeeee“ muss dabei durch den 20stelligen Aktivierungscode für ActiveInspire ersetzt werden.</p>	C:\ProgramData\Promethean\ActivInspire
Budenberg	<p>lizenz.cfg</p> <p>Die notwendige Datei wird durch den Softwarehersteller bei vorhandener Lizenz bereitgestellt. Die vorhandene Demo-Lizenzdatei im Zielordner muss dabei überschrieben werden.</p>	C:\Budenberg
Lernwerkstatt 10 (lokale Installation)	<p>vlws.dem</p> <p>Bei der lokalen Installation befinden sich neben den Programmdateien auch die Dateien der Datenablage (ca. 5 GB) auf dem Endgerät. Die Lizenzdatei kann durch manuelles Eingeben der Lizenzdaten in der Lernwerkstatt an einem Endgerät erstellt werden und befindet sich dann im angegebenen Zielordner.</p>	C:\ProgramData\LWX DaAb
Lernwerkstatt 10 (Netzwerkinstallation)	<p>Datenablagepfad.txt</p> <p>Bei der Netzwerkinstallation befinden sich nur die Programmdateien auf dem Endgerät. Die Datenablage (ca. 5 GB) wird auf einem Netzwerklaufwerk in der Schule zur Verfügung gestellt. Im Netzwerkpfad muss die Lizenzdatei (vlws.dem) für alle Geräte abgelegt werden. Diese wird dort automatisch angelegt, wenn an einem Gerät mit eingestelltem Netzwerkpfad die Lizenzdaten manuell eingegeben werden. Durch das Kopieren der Datei "Datenablagepfad.txt", die den Zielpfad der Lernwerkstatt-Datenablage enthalten muss, in den Programmpfad auf den Endgeräten, wird auch die Lizenzierung der Endgeräte vorgenommen. Die Nutzung der Lernwerkstatt ist jedoch nur innerhalb dieses Netzwerks möglich.</p>	C:\Program Files (x86)\Lernwerkstatt 10
Worksheetcraft er	<u>Bei der Nutzung einer aktuellen Lizenz:</u>	

	<p>Beim aktuellen Lizenz-Modell erhalten eingetragene Lehrkräfte persönliche Lizenzdaten. Die Eingabe erfolgt dann manuell am jeweiligen Endgerät durch die Lehrkraft.</p> <p><u>Bei Nutzung einer alten Schullizenz:</u> admin.ini Die Datei erhält man durch Umbenennung der Datei admin.ini.sample im Programmordner. Unter dem Abschnitt "License" muss der Lizenzcode und die zugehörige Mailadresse hinterlegt werden: <i>[License]</i> <i>UserName=meinemail@mail.de</i> <i>LicenseCode=XXXX-XXXX-XXXX-XXXX</i></p>	<p>C:\Program Files (x86)\Worksheet Crafter</p>
--	--	--

14.6 Paketierung Microsoft Office

Da Microsoft Office an vielen Schulen eingesetzt wird, sollen in diesem Teilkapitel die notwendigen Schritte zur Paketerstellung für diese Software erklärt werden.

14.6.1 Microsoft Office 2016

Zunächst muss eine MSP-Konfigurationsdatei erstellt werden. Dazu die ISO-Installationsdatei für Microsoft Office 2016 entpacken.

Über die Windows-Eingabeaufforderung im entpackten Installationsordner mit nachfolgendem Befehl das Microsoft Office-Anpassungstool starten: `setup.exe /admin`.

Eine neue Setupanpassungsdatei mit folgende Einstellungen erstellen:

- Office Open XML-Format auswählen.
- Lizenzierung:
 - Volumen-Lizenzschlüssel eintragen.
 - Vertragsbedingungen zustimmen.
 - Anzeigeebene:
 - Anzeigeebene auf „Keine“ stellen.
 - „Abschlusshinweis“ und „Kein Abbrechen“ deaktivieren.
 - „Modalen Modus unterdrücken“ aktivieren.
- Setup-Eigenschaften ändern:
 - Zwei Eigenschaften hinzufügen:
 - Name: HIDEUPDATEUI, Wert = True
 - Name: SETUP_REBOOT, Wert = Never
- Featureinstallationsstatus festlegen:
 - Microsoft OneDrive for Business deaktivieren („Nicht verfügbar“).
 - Microsoft Outlook deaktivieren („Nicht verfügbar“).

Über „Datei“ – „Speichern unter“ die MSP-Datei im Installationsordner „updates“ abspeichern.

Alle Ordner und Dateien der ISO-Installation inklusive der MSP-Datei im Unterordner „updates“ mit 7ZIP in eine ZIP-Datei packen.

Die ZIP-Datei wie im Kapitel [Paket-Erstellung](#) beschrieben im UEM hochladen und als Paket konfigurieren. Als Installationsbefehl reicht es aus „setup.exe anzugeben. Die Konfiguration der MSP-Datei wird dann automatisch abgerufen, da diese im Ordner „updates“ liegt.

Hinweis: Beim Installieren des Paketes wird die gesamte Installation im Hintergrund ausgeführt. Beim ersten Programmstart muss die hinterlegte Lizenz einmalig über das Internet aktiviert werden.

14.6.2 Microsoft Office 2019 und 2021

Bevor das Paket für Microsoft Office erstellt werden kann, muss eine Konfigurationsdatei angelegt werden. Diese kann über zwei Wege erstellt werden:

- Variante 1: Unter <https://config.office.com/deploymentsettings> kann eine individuelle Konfiguration für Microsoft Office (z. B. Aktivierung/Deaktivierung bestimmter

Teilprogramme) vorgenommen werden und die zugehörige Konfigurationsdatei heruntergeladen werden.

- Variante 2: Es wird die von uns erstellte Konfigurationsdatei (XML-Datei) verwendet, welche Sie im ZIP-Verzeichnis unter <https://medienberatung.iqsh.de/endgeraete-lk-st-anl-videos.html> herunterladen können.

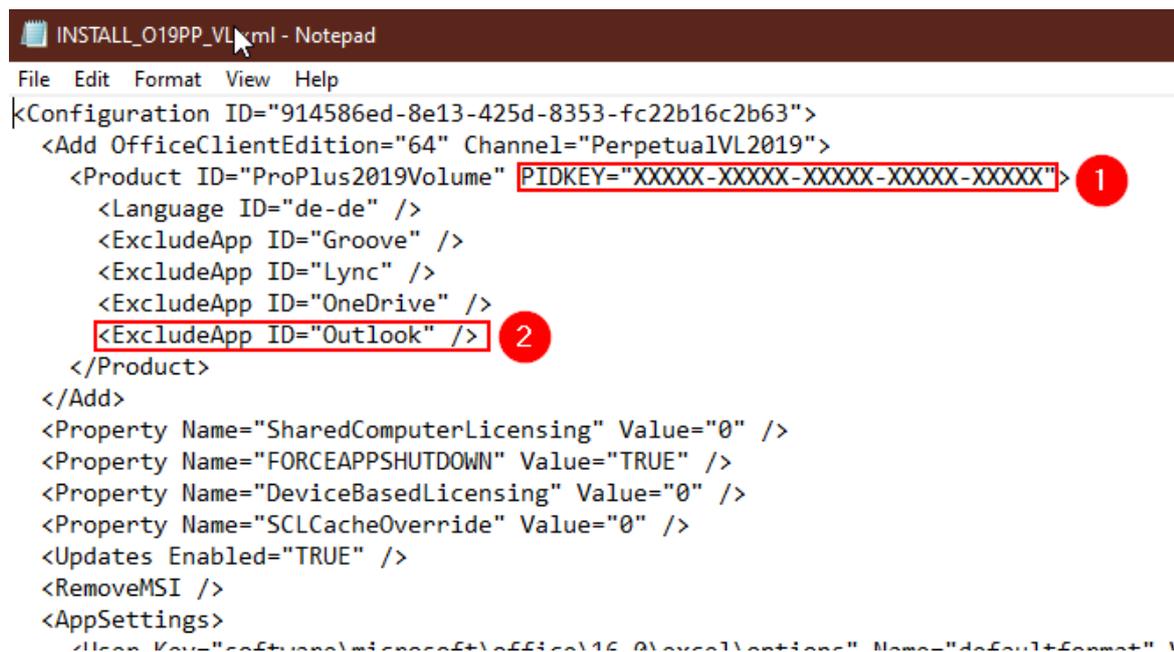
Bei Nutzung der Variante 2:

Die XML-Datei muss zunächst für die eigene Verwendung angepasst werden. Dazu extrahieren Sie das ZIP-Paket. In diesem Ordner finden Sie eine Vielzahl an Dateien. Einerseits die „setup.exe“ als auch diverse XML-Konfigurationsdateien. Je nachdem, welche Microsoft Office-Version und Lizenz verwendet wird, muss eine andere XML-Datei für das eigene Paket verwendet werden.

Die Namen der XML-Dateien sind wie folgt aufgebaut:

INSTALL- (Installation-Konfiguration) oder **UNINSTALL-** (Deinstallation-Konfiguration) **O19** (Office 2019) oder **O21** (Office 2021) **PP** (ProPlus) oder **STD** (Standard) **_VL** (Volumenlizenz).

Dementsprechend muss für die Verwendung von Office 2019 ProPlus die INSTALL_O19PP_VL.xml editiert werden. Dazu wird die XML-Datei geöffnet:



```

INSTALL_O19PP_VL.xml - Notepad
File Edit Format View Help
<Configuration ID="914586ed-8e13-425d-8353-fc22b16c2b63">
  <Add OfficeClientEdition="64" Channel="PerpetualVL2019">
    <Product ID="ProPlus2019Volume" PIDKEY="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"> 1
      <Language ID="de-de" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="Lync" />
      <ExcludeApp ID="OneDrive" />
      <ExcludeApp ID="Outlook" /> 2
    </Product>
  </Add>
  <Property Name="SharedComputerLicensing" Value="0" />
  <Property Name="FORCEAPPSHUTDOWN" Value="TRUE" />
  <Property Name="DeviceBasedLicensing" Value="0" />
  <Property Name="SCLCacheOverride" Value="0" />
  <Updates Enabled="TRUE" />
  <RemoveMSI />
  <AppSettings>
    <User Key="software\microsoft\office\16.0\apps\options" Name="defaultformat" V
  
```

Unter „PIDKEY=“ (1) wird der Lizenzschlüssel angegeben und sofern Outlook installiert werden soll, muss die Zeile mit der Markierung (2) (ExcludeApp ID=“Outlook“) entfernt werden.

Hinweis: Die Komponenten Skype for Business, Microsoft Teams oder OneDrive müssen aus datenschutzrechtlichen Gründen deaktiviert bleiben.

Anschließend muss ein ZIP-Archiv erstellt werden, welches die Datei „setup.exe“, die Installationskonfiguration und die Deinstallationskonfiguration der jeweiligen Office- Version enthält.

Die Paketierung des Office-Pakets basiert auf den Schritten aus dem Kapitel [Paket-Erstellung](#). Dort wird das soeben erstellte ZIP-Archiv hochgeladen. Als Installationsbefehl wird „setup.exe /configure Installation-Konfigurationsdatei“ angegeben. Der Name der Installation-Konfigurationsdatei entspricht der XML-Datei, die in der ZIP-Datei enthalten ist. In unserem Beispiel wäre es „setup.exe /configure INSTALL_O19PP_VL.xml“.

Als Deinstallationsbefehl wird „setup.exe /configure Deinstallation-Konfigurationsdatei“ angegeben. In unserem Beispiel wäre es „setup.exe /configure UNINSTALL_O19PP_VL.xml“.

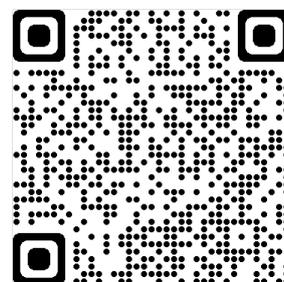
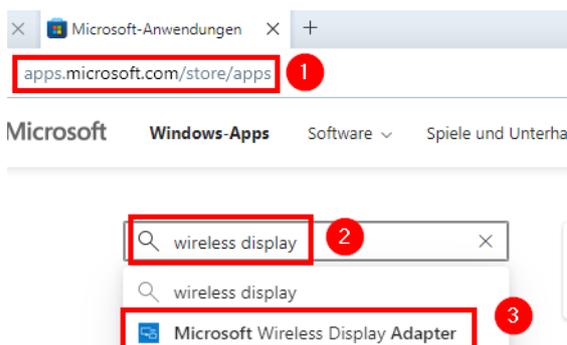
Die restlichen Schritte folgen der Anleitung aus dem Kapitel [Paket-Erstellung](#).

Hinweis: Wählen Sie ein geeignetes Prüfkriterium für den Abschluss der Installation (siehe Bereitstellungsmöglichkeiten). Andernfalls wird die App unmittelbar nach Abschluss der Installation wieder entfernt.

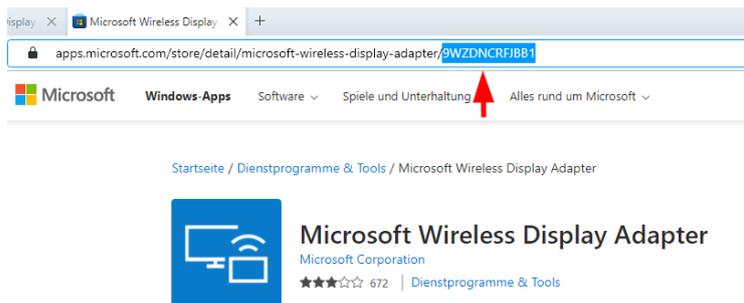
14.7 Paketierung Microsoft-Store-App

Für die Paketierung einer App aus dem Microsoft Store wird zunächst die zugehörige App-ID benötigt. Diese erhält man auf folgendem Weg:

- Webseite des Microsoft Stores über die Adresse <https://apps.microsoft.com/store/apps> aufrufen (1), über die Suchfunktion die zu installierende App suchen (2) und die zugehörige App-Detailseite öffnen (3):



- Aus der Adresszeile der nun angezeigten App-Detailseite die App-ID herauskopieren. Diese befindet sich am Ende der Webadresse und beginnt hinter dem letzten Schrägstrich:

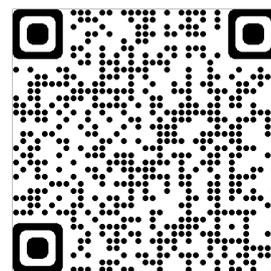


Beispiel: <https://apps.microsoft.com/store/detail/microsoft-wireless-display-adapter/9WZDNCRFJBB1>

Hinweis: Wenn die App über eine Suchmaschine bzw. über die Seite <https://www.microsoft.com> gesucht wird, enthält der Link zur App noch einen zusätzlichen Teil hinter der App-ID. In diesem Fall befindet sich die App-ID zwischen dem letzten Schrägstrich und dem ersten Fragezeichen des Links: <https://apps.microsoft.com/store/detail/microsoft-wireless-display-adapter/9WZDNCRFJBB1?hl=de-de&gl=DE>

Im Anschluss die Datei „MicrosoftStoreApp.zip“ von der Seite <https://medienberatung.iqsh.de/endgeraete-ik-st-anl-videos.html> herunterladen. Das ZIP-Archiv enthält folgende Dateien:

- InvokeStoreInstall.ps1: Powershell-Skript, das die App-Installation durchführt
- CheckInstall.ps1: Powershell-Skript, das nach der Installation überprüft, ob die App auf dem Gerät korrekt installiert wurde
- InvokeAppUninstall.ps1: Powershell-Skript, das die App-Deinstallation durchführt
- Dummy.exe: Ohne die diese Datei lässt sich die ZIP-Datei nicht ins UEM hochladen. Im ZIP-Archiv verlangt das UEM zwingend eine ausführbare Datei. Diese hat sonst keine Funktion.



Achtung: Bedingt durch eine zwischenzeitlich eingeführte Hash-Prüfung der hochgeladenen Dateien, muss die Zip-Datei für jede App neu erstellt werden!

Im UEM wie in Kapitel [Paket-Erstellung](#) beschrieben eine Anwendung mit folgenden Einstellungen hinzufügen:

- App-Datei: MicrosoftStoreApp.zip (siehe oben)
- Deinstallationsbefehl: powershell.exe -executionpolicy bypass -file .\InvokeAppUninstall.ps1 **9WZDNCRFJBB**
Hinweis: Den gelb markierten Teil durch die App-ID der zu installierenden App (siehe oben) austauschen.
- Installationsbefehl: powershell.exe -executionpolicy bypass -file .\InvokeStoreInstall.ps1 **9WZDNCRFJBB1**
Hinweis: Den gelb markierten Teil durch die App-ID der zu installierenden App (siehe oben) austauschen.
- Im Bereich „Wann Installation abgeschlossen ist“ das benutzerdefinierte Skript aktivieren (1) und folgende Einstellungen vornehmen:

Wann Installation abgeschlossen ist

ⓘ

Identifizierung der Anwendung nach* DEFINIERENDE KRITERIEN **UNTER VERWENDUNG VON BENUTZERDEFINIERTEM SKRIPT** ⓘ

Skripttyp* PowerShell ⓘ **2**

Befehl zum Ausführen des Skriptes powershell.exe -executionpolicy bypass -file .\CheckInstall.ps1 9WZDNCRFJBB1 ⓘ **3**

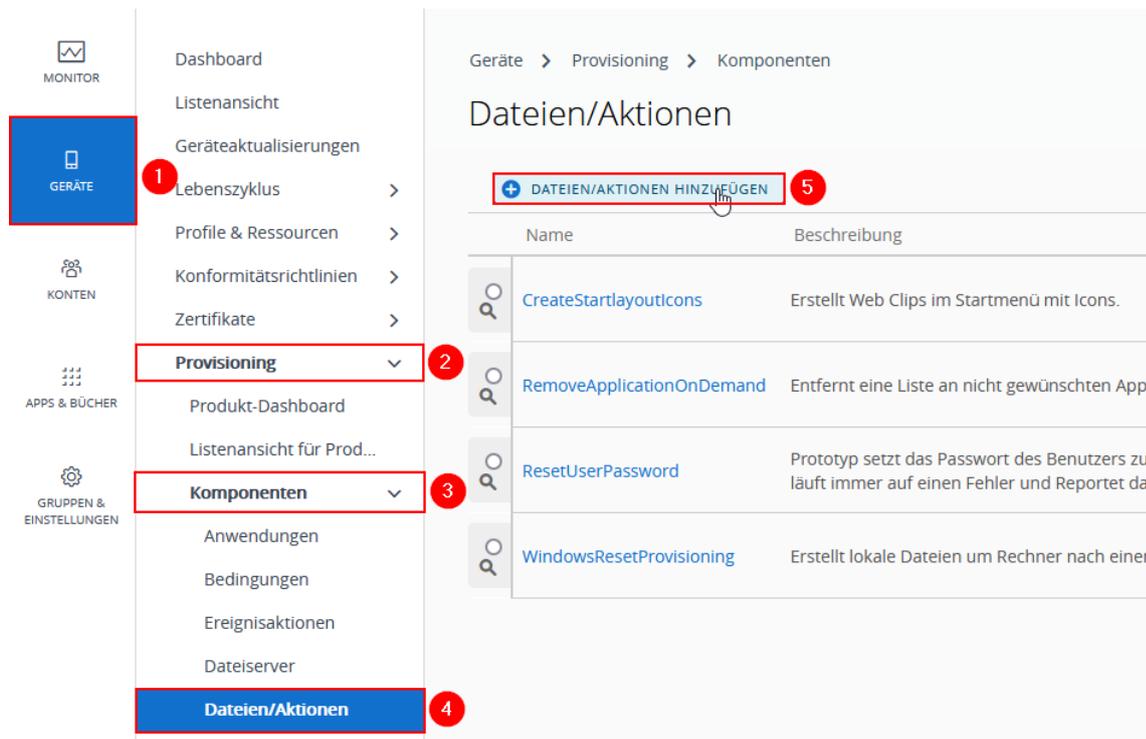
Benutzerdefinierte Skriptdatei CheckInstall.ps1 ⓘ **4**

Erfolg - Exitcode 0 ⓘ **5**

- Skripttyp (2): Powershell
- Skriptbefehl (3): powershell.exe -executionpolicy bypass -file .\CheckInstall.ps1 **9WZDNCRFJBB1**
Hinweis: Den gelb markierten Teil durch die App-ID der zu installierenden App (siehe oben) austauschen.
- Skriptdatei (4): Checkinstall.ps1
Hinweis: Die Datei muss aus dem ZIP-Archiv „MicrosoftStoreApp.zip“ entpackt und hier hochgeladen werden.
- Exitcode (5): 0

15 Windows: Kopieren von Dateien/Ordnern

Um eine Datei zu verteilen zu können, muss im UEM die passende Organisationseinheit (z. B. Schulträger) gewählt werden, unter „Geräte“ (1) - „Provisioning“ (2) - „Komponenten“ (3) den Reiter „Dateien/Aktionen“ (4) wählen. Anschließend auf „Dateien/Aktionen hinzufügen“ (5) klicken:



Daraufhin „Windows“ und „Windows-Desktop“ auswählen:

Dateien/Aktionen hinzufügen

Gerätetyp auswählen



Im nächsten Fenster unter „Allgemein“ (1) einen Namen (2) (nach folgendem Schema vergeben: GroupID (SH001), Bindestrich, Schulname, Datei/Dateiname) für die Datei eingeben. Die Organisation (3) wird automatisch ausgefüllt:

Dateien/Aktionen hinzufügen

Allgemein **1** Dateien Manifest

Name * **2** SH001-Musterschule-Fernwartung

Beschreibung

Version 1 **1**

Plattform Windows Desktop

Verwaltet von * **3** TSchultraeger SVS L

Anschließend unter „Dateien“ (1) die „Dateien hinzufügen“ (2):

Dateien/Aktionen hinzufügen

Allgemein **Dateien** **1** Manifest

+ DATEIEN HINZUFÜGEN **2**

Dateiname

Mittels „Durchsuchen“ (1) auswählen. Der Dateiname wird nach der Auswahl neben „Durchsuchen angezeigt“. Anschließend mit „Speichern“ (2) bestätigen:

Dateien hinzufügen ×

Datei **1** Durchsuchen... fernwa...g.exe
 hinzufügen*

2 **SPEICHERN** ABBRECHEN

Daraufhin den Zielpfad (1) auf dem Gerät für die Datei angeben und mit „Speichern“ den Vorgang abschließen:

Dateien hinzufügen ×

Datei - 1

Name

Downloadpfad * 1

Version *

Bei Bedarf die Schritte zur Entfernung der Datei angeben. Dazu unter „Manifest“ (1) im Bereich „Manifest deinstallieren“ die „Aktion hinzufügen“ (2):

Dateien/Aktionen hinzufügen

Allgemein Dateien **Manifest** 1

Manifest installieren

+ AKTION HINZUFÜGEN

Aktiv	Runter	Schrittnummer	Aktionstyp	Beschreibung
▲	▼	1	Ordner erstellen	Pfad = C:\Schule\

Elemente 1-1 von 1

Manifest deinstallieren

+ AKTION HINZUFÜGEN 2

Aktiv	Runter	Schrittnummer	Aktionstyp
-------	--------	---------------	------------

Anschließend die „Auszuführende Aktion(en)“ auswählen (1) und den Pfad (2) für die jeweilige Aktion angeben und mit „Speichern“ bestätigen:

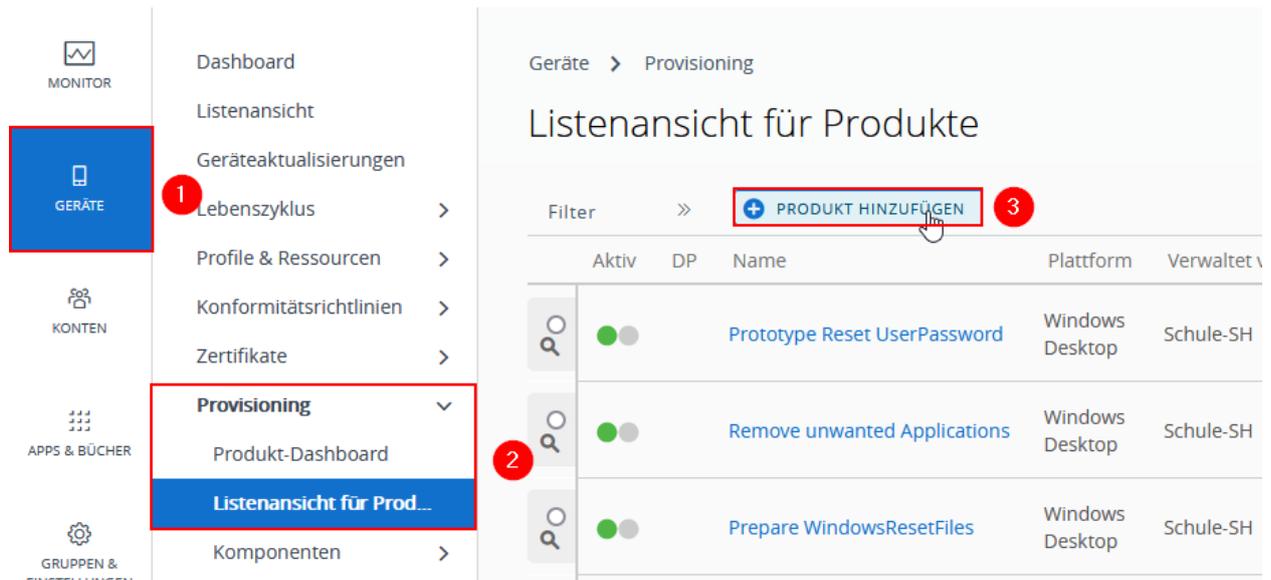
Manifest hinzufügen ×

Auszuführende Aktion(en) * Dateien löschen 1

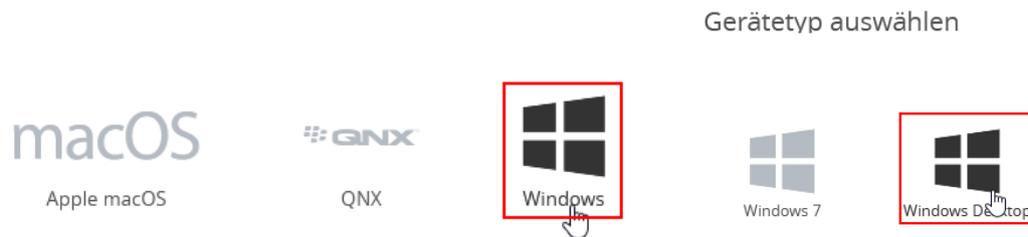
Pfad und Name der Datei, die gelöscht werden soll * C:\Schule\fernwartung.exe 2

Um die Datei im UEM zu speichern auf „Speichern“ klicken“.

Daraufhin muss die Datei noch zugewiesen werden. Dafür unter „Geräte“ (1) - „Provisioning“ - „Listenansicht für Produkte“ (2) auf „Produkt hinzufügen“ (3) klicken:



Daraufhin „Windows“ und „Windows-Desktop“ auswählen:



Im „Reiter“ (1) den Namen für die Zuweisung (nach folgendem Schema vergeben: GroupID (SH001), Bindestrich, Schulname, Datei/Dateiname, Gruppe) angeben (2) und die Zuweisungsgruppe (3) auswählen:



Damit die Datei zur Zuweisung zugeordnet wird im Reiter „Manifest“ (1) die Datei mittels „Hinzufügen“ (2) auswählen:

Produkt hinzufügen

Allgemein **Manifest** 1 Bedingungen Bereitstellung Abhängigkeiten

+ HINZUFÜGEN 2

Aktiv	Runter	Schrittnummer	Aktionstyp	Persistent
-------	--------	---------------	------------	------------

Im Fenster die „Auszuführende Aktion(en)“ (1) auswählen. Zum Zuweisen der Datei „Datei/Aktion – Installieren“ auswählen. Zum Entfernen auf „Datei/Aktion – Deinstallieren“ klicken. Anschließend die zuvor angelegte Datei (2) auswählen und mit „Speichern“ bestätigen:

Manifest hinzufügen ×

Auszuführende Aktion(en) * 1 Datei/Aktion – Installieren

Dateien/Aktionen * 2 SH001-Musterschule-Fernwartung

Um die Zuweisung abzuschließen auf „Aktivieren“ klicken, worauf Sie eine Übersicht aller zugewiesenen Geräte erhalten (1). Mit „Aktivieren“ (2) abschließend bestätigen:

Gerätezuweisung anzeigen



 **EXPORTIEREN**

Zuweisungsstatus	Anzeigenname	Benutzer	Plattform/BS/Modell	Rufnummer	Organisationsgruppe

1

< > Elemente 1 – 1 von 1 Seitengröße: 50

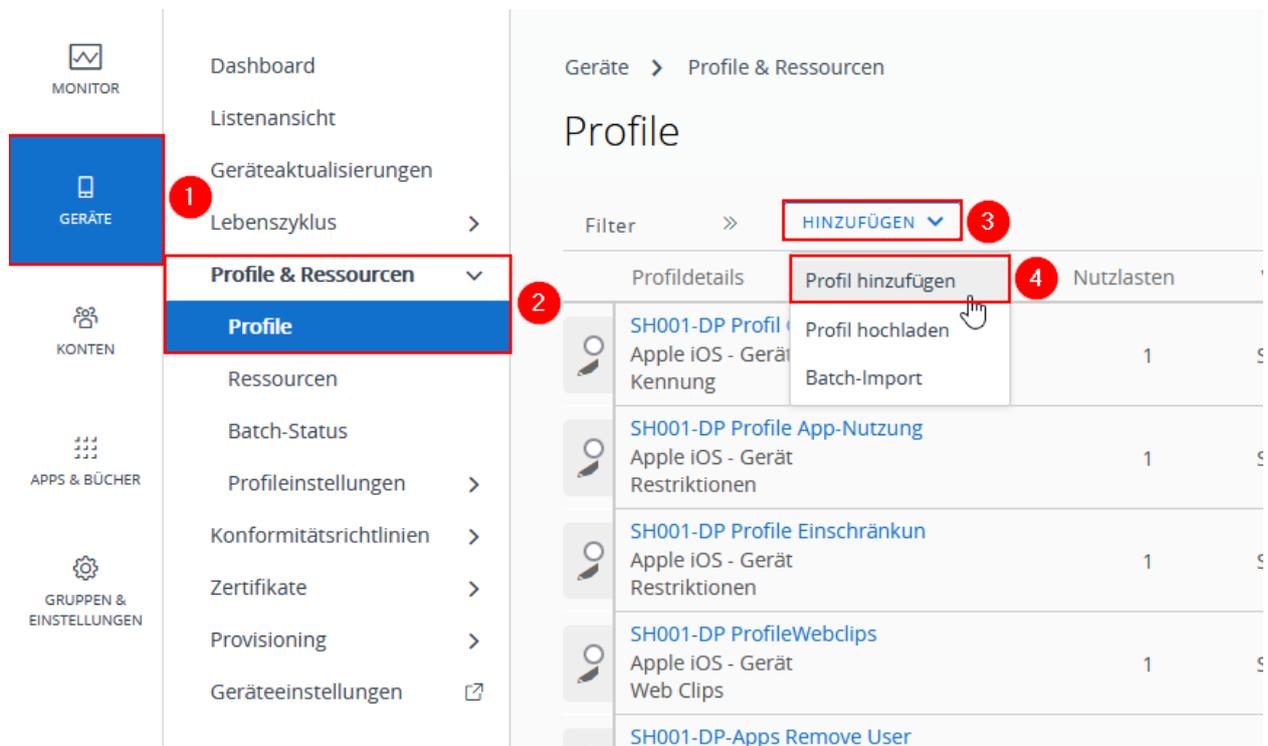
2 **AKTIVIEREN** **ABBRECHEN**

16 Windows: Profil erstellen

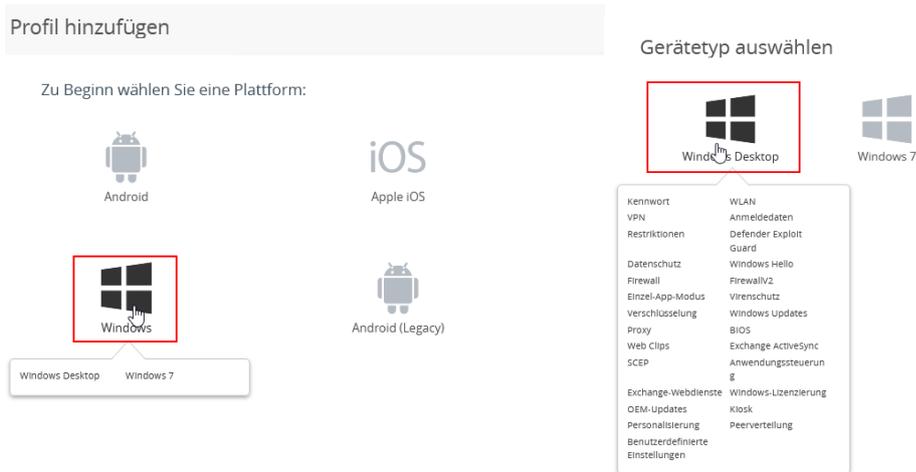
Empfehlung: Um später mögliche Fehlerquellen besser identifizieren zu können, sollte man Profile nicht zu umfangreich gestalten und möglichst auf einen Aspekt (z. B. WLAN-Einstellungen, Webclips usw.) reduzieren.

Ein Profil wird über folgende Schritte erstellt:

Im Menü „Geräte“ (1) - „Profile & Ressourcen“ - „Profile“ (2) - „Hinzufügen“ (3) - „Profil hinzufügen“ (4) wählen:



Als Plattform „Windows“ und „Windows Desktop“ wählen:



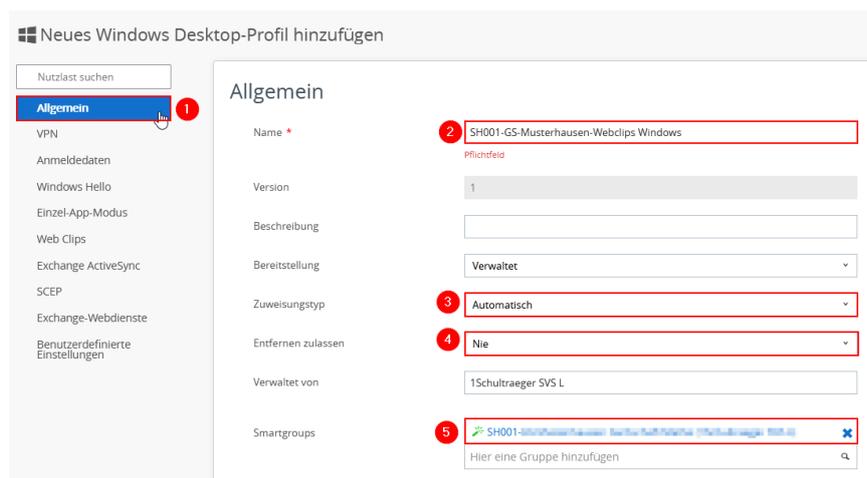
„Benutzerprofil“ wählen:

Kontext wählen



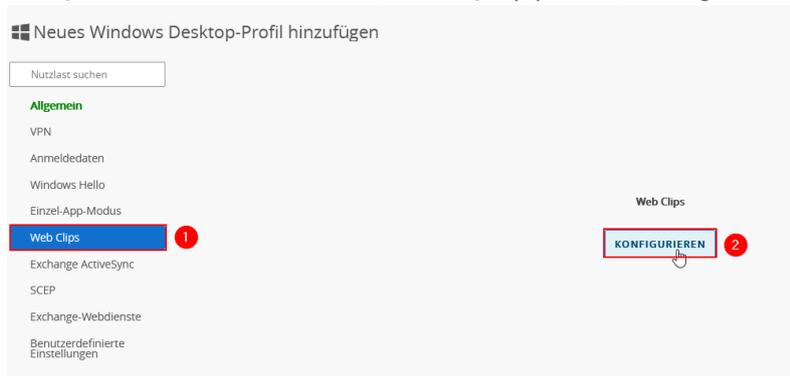
Unter „Allgemein“ folgende Eintragungen/Einstellungen vornehmen:

- Profilnamen nach folgendem Schema vergeben: GroupID (SH001), Bindestrich, Schulname, Profilname (z. B. SH001-GS Musterhausen Webclips Windows).
- Zuweisungstyp (automatisch oder optional) auswählen.
- „Entfernen zulassen“ auf „Nie“ einstellen.
- Passende Smartgroup auswählen.

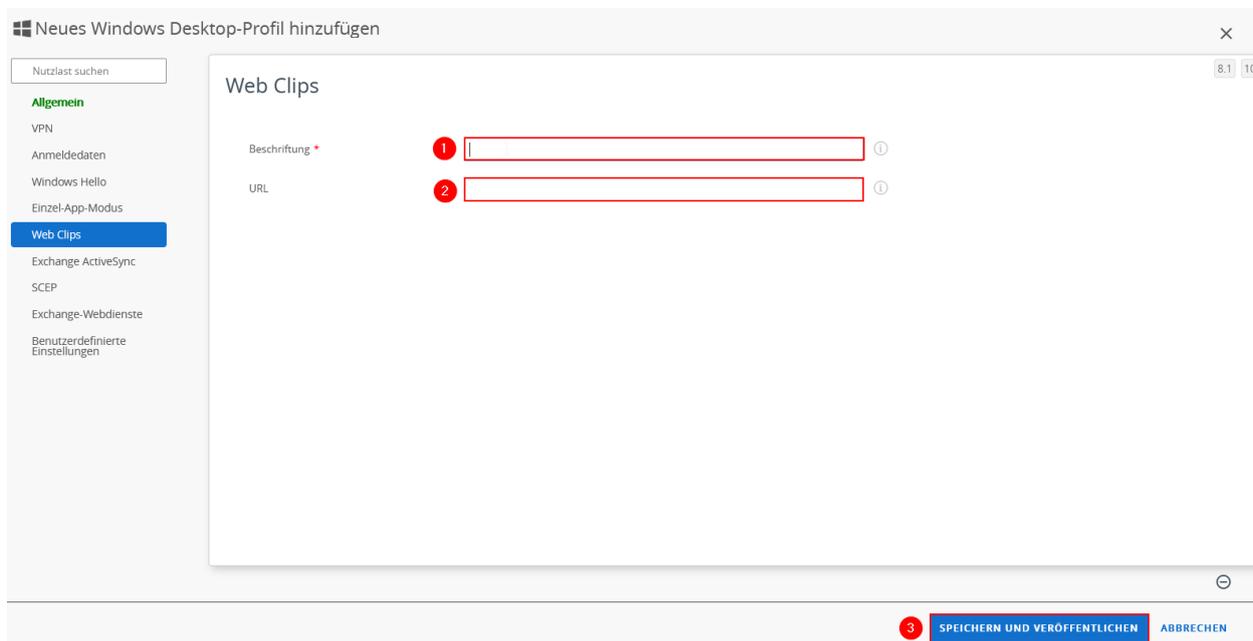


Über das Auswahlménü können nun unterschiedliche Einstellungen hinzugefügt werden, zum

Beispiel kann ein Link unter „Webclip“ (1) über „Konfigurieren“ (2) hinzugefügt werden:

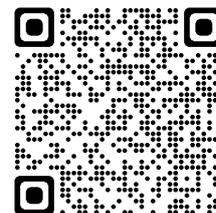


Nach Eingabe der Beschriftung (1) und der Webadresse (2) kann das Profil über „Speichern und Veröffentlichen“ (3) zugewiesen werden:



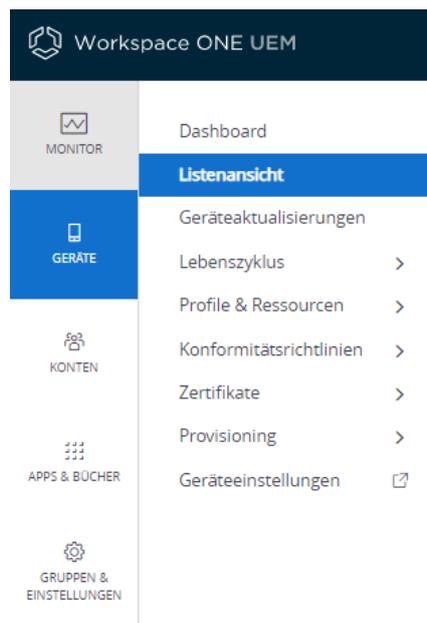
17 Windows: Passwort oder Endgerät zurücksetzen

Das Zurücksetzen des Gerätepasswortes oder des Endgerätes kann durch dezentrale Administratoren und Administratorinnen (Schulträger, Dienstleister, RBZ/BBS) oder Dataport erfolgen. Das folgende Kapitel beschreibt die Vorgehensweise für die dezentralen Administratoren und Administratorinnen. Soll das Zurücksetzen über Dataport erfolgen, so ist durch die betroffene Lehrkraft oder die Schulleitung ein Ticket über das Helpdesk-Formular unter <https://www.secure-lernetz.de/helpdesk> im Bereich „LK-Endgeräte“ – „Support“ zu eröffnen.



Hinweise:

- Beide Funktionen nutzen ein zentral verteiltes Tool. Die erfolgreiche Installation des Tools auf dem Endgerät wird auf dem Anmeldebildschirm durch die Verfügbarkeit der „Anmeldeoptionen“ erkennbar. (siehe DataportResetTool)
- Die Funktionalität auf dem Endgerät entnehmen Sie bitte dem Handbuch für Windows-Endgeräte. <https://medienberatung.igsh.de/endgeraete-lk-s-anl-videos.html>



Zur Vorbereitung der in der Folge beschriebenen Schritte wechseln Sie in die Listenansicht im Bereich „Geräte“ und selektieren dort das betroffene Gerät.

Hinweis: Sind sehr viele Geräte für Ihre Schule/Ihren Schulträger registriert, empfiehlt sich die Verwendung der Suchfunktion (Eingabefeld „Liste durchsuchen“). Hier kann sowohl über die Seriennummer als auch über den Namen der Lehrkraft oder Benutzerkennung gesucht werden.

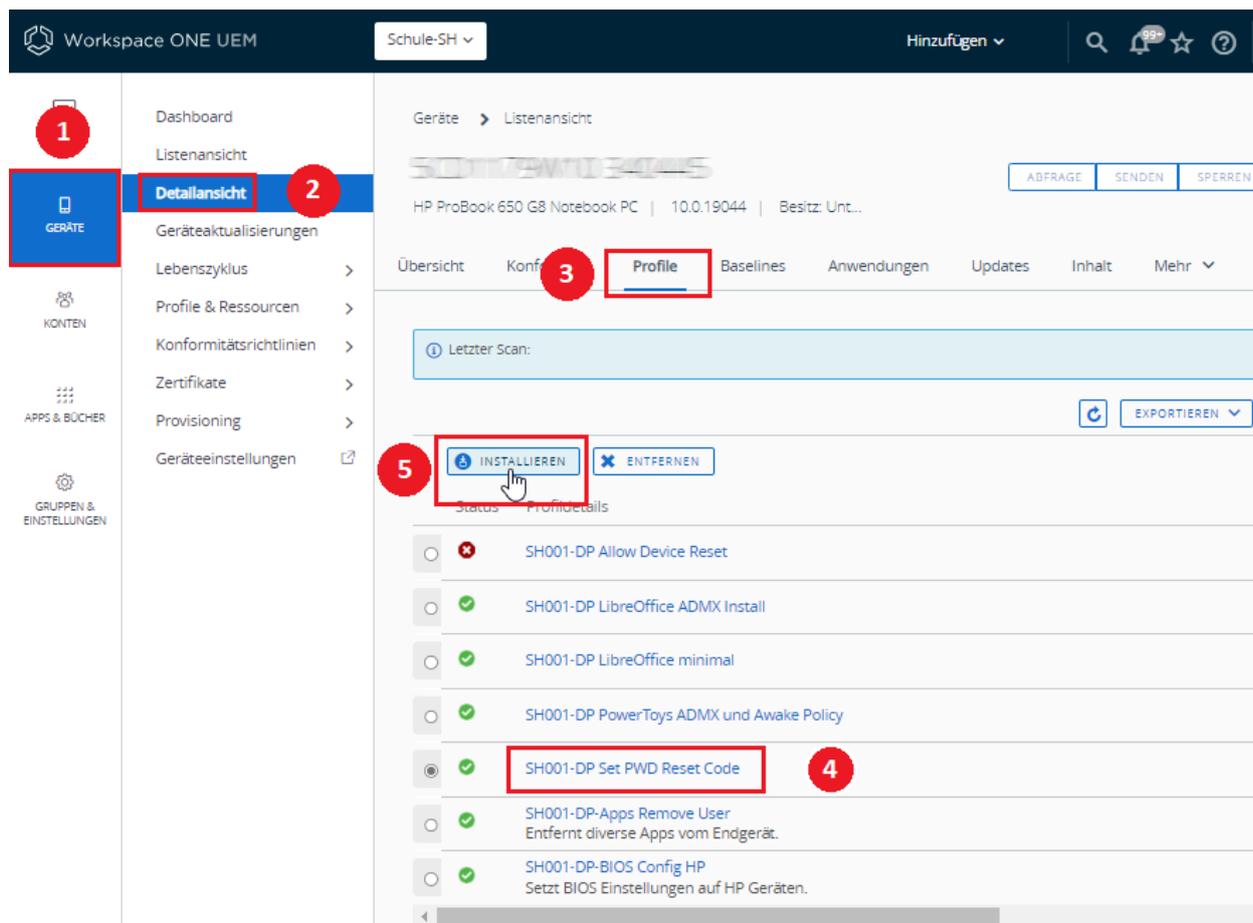
Klicken Sie auf die in „Allgemeine Informationen“ verlinkte Geräteerkennung (i.d.R. Seriennummer + Inventarnummer), um in die Detailansicht des Gerätes zu wechseln.

Zuletzt gesehen	Allgemeine Info	Plattform	Benutzer
45 s	SCD1179W10 [Redacted] Von UEM verwaltet Unternehmen - Dediziert	Windows Desktop HP ProBook 650 G8 Notebook PC 10.0.19044	Dennis E DBrady+ Dennis E

17.1 Windows Passwort zurücksetzen

Die benötigten Funktionen sollten bereits auf den Endgeräten verfügbar sein, das Zurücksetzen muss jedoch durch UEM-Administratorinnen oder Administratoren autorisiert werden. Das erfolgt durch Installation eines Profils.

Für das Zurücksetzen wird das Profil „SH001-DP Set PWD Reset Code“ (4) benötigt. Die Freigabe erfolgt indem das Profil über die Radiobox selektiert und anschließend installiert (5) wird.

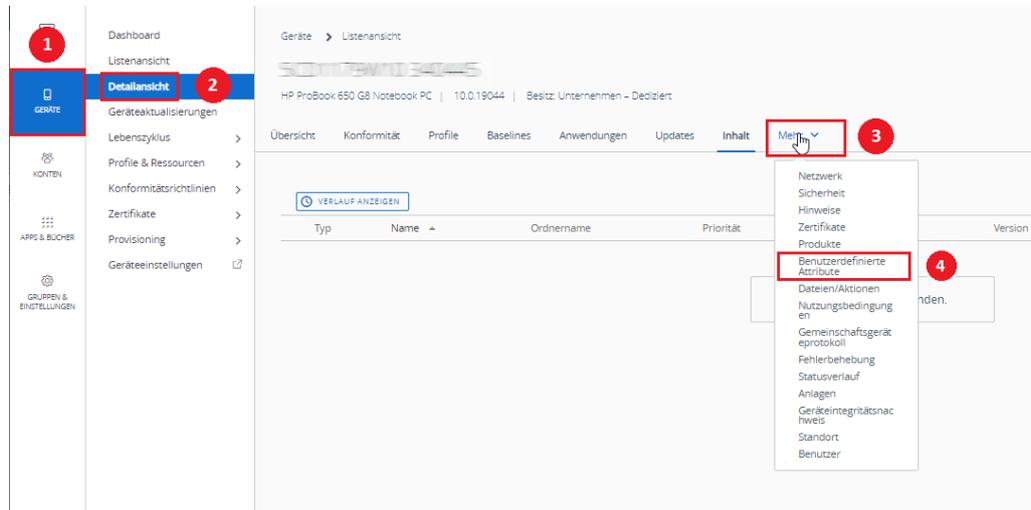


Hinweise:

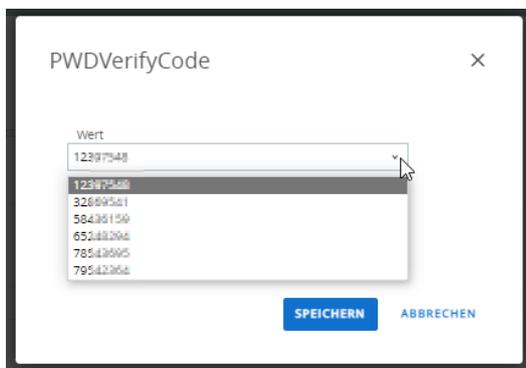
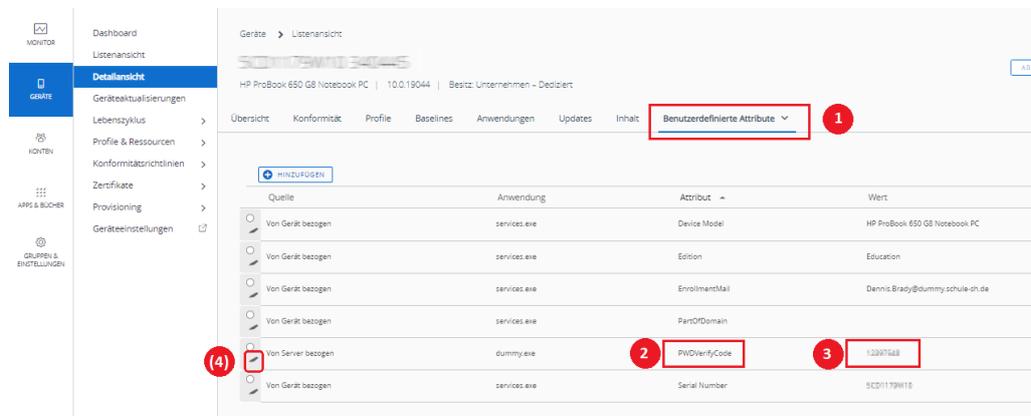
- Startet die Lehrkraft den Prozess auf Ihrem Endgerät bleibt das Profil installiert (Status: ) , wird jedoch deaktiviert. Vor einem neuen Versuch muss das Profil neu installiert werden.
- Die Freigabe ist zeitlich befristet. Startet die Lehrkraft den Vorgang innerhalb einer vordefinierten Frist nicht, wird das Profil automatisch deaktiviert und muss ggf. neu installiert werden.
- Sollte das Profil nicht verfügbar sein, bitte den Tag „LK-PasswordReset“ aktivieren.

Für das Zurücksetzen des Passwortes und die Generierung des temporären Passwortes benötigt die Lehrkraft einen Freigabe-PIN. Dieser 8-stellige PIN ist als Benutzerdefiniertes Attribut in den Detailinformationen des Gerätes hinterlegt und muss der Lehrkraft übermittelt werden.

Die „Benutzerdefinierten Attribute“ (4) finden sich in der Detailansicht (2) unter „Mehr“ (3).



Der Freigabe-PIN ist als Attribut „PWDVerifyCode“ (2) angelegt. Der gültige PIN kann unter (3) ausgelesen werden.

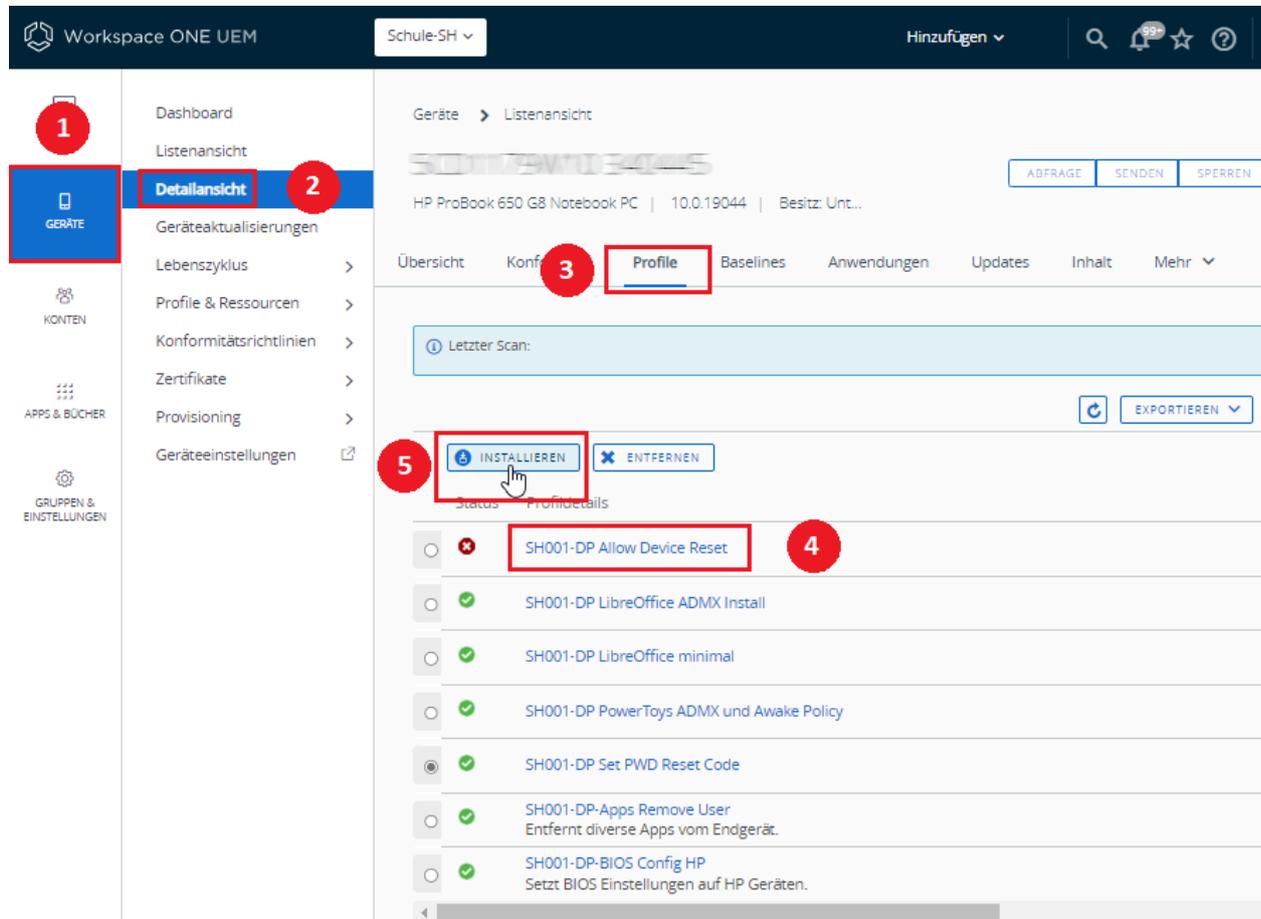


Unter (4) besteht die Möglichkeit einen anderen PIN aus einer Liste vordefinierter PINs auszuwählen.

Hinweis: Die PIN-Liste wird regelmäßig automatisch ausgetauscht um eine Wiederverwendung bekannter Werte zu verhindern.

17.2 Windows: Gerät zurücksetzen

Das Zurücksetzen eines Windows-Endgerätes muss durch UEM-Administratorinnen und Administratoren freigegeben werden. Dies erfolgt - wie beim Zurücksetzen des Passwortes – durch Installation eines Profils, in diesem Fall des Profils „SH001-DP Allow Device Reset“ (4).

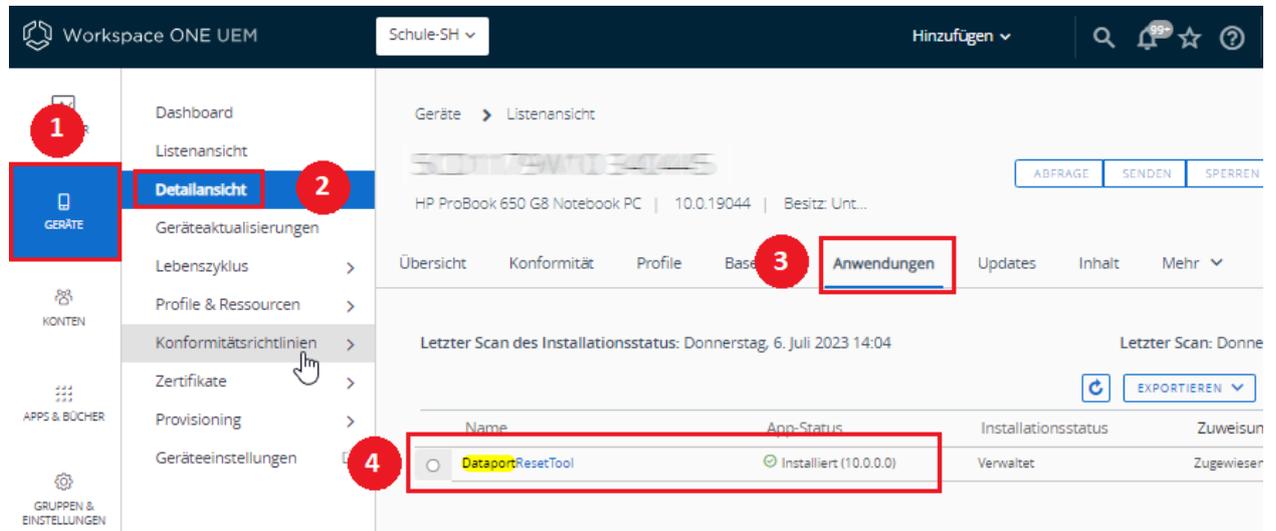


Hinweise:

- Die Freigabe ist zeitlich befristet. Startet die Lehrkraft den Vorgang innerhalb einer vordefinierten Frist nicht, wird das Profil automatisch deaktiviert und muss ggf. neu installiert werden.
- Sollte das Profil nicht verfügbar sein, bitte den Tag „LK-DeviceReset“ aktivieren.

17.3 DataportResetTool

Sollten die Anmeldeoptionen auf dem betroffenen Endgerät nicht verfügbar sein, dann sollte der Installationsstatus des DataportResetTools (4) in den in der Detailansicht (2) verfügbaren Anwendung (3) geprüft werden.



18 Windows: Netzlaufwerk verteilen

Hinweis: Das Verteilen von Netzlaufwerken wird in diesem Kapitel beispielhaft über die Installation der im Hub zur Verfügung gestellten Software „MyDriveControl“ sowie der Verteilung einer zugehörigen Konfigurationsdatei erklärt. Alternativ dazu wäre auch das Verteilen eines Netzlaufwerkes mit Hilfe eines Skriptes möglich. Soll zusätzlich zum Pfad des Netzlaufwerks auch Benutzername und Kennwort verteilt werden, wäre dazu die Nutzung eines Powershell-Skriptes und einer verschlüsselten Passwortdatei notwendig. Die bloße Bereitstellung über den Befehl „net use“ wäre hier nicht ausreichend, da Zugangsdaten im Klartext übermittelt und nicht auf dem Endgerät abgespeichert werden.

Mit Hilfe der Software MyDriveControl können Lehrkräfte manuell Netzwerklauferwerke (SMB und WebDAV) auf ihrem Endgerät verbinden. Mit Hilfe einer Konfigurationsdatei, die über das UEM auf die Endgeräte verteilt wird, können die Netzlaufwerke jedoch auch vorgegeben werden. Die Software „MyDriveControl“ kann dabei sowohl vor als auch nach der Verteilung der Konfigurationsdatei auf den Endgeräten installiert werden.

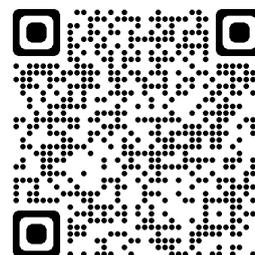
Bei der Bereitstellung der Konfiguratuionsdatei unterscheidet man zwei Varianten voneinander:

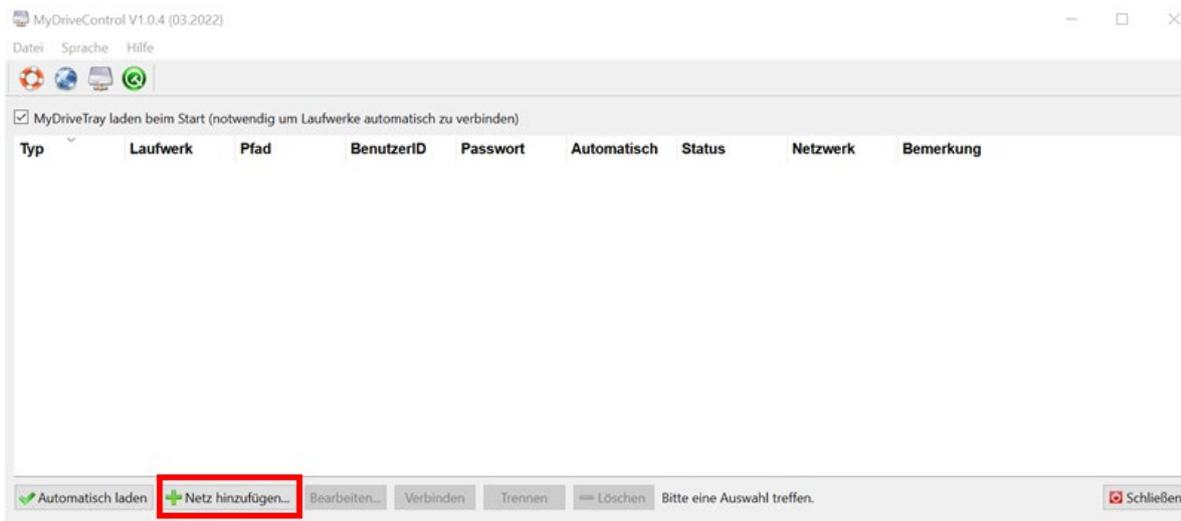
- **Variante 1** (CFG-Datei): Die Variante eignet sich zum Verteilen von Netzlaufwerken, die bereits inklusive der Zugangsdaten auf den Lehrkräfte-Geräten eingerichtet werden sollen. Die Konfigurationsdatei wird mit Hilfe der Software MyDriveControl erstellt, indem hier einmalig die zu verteilenden Netzlaufwerke angelegt werden. Das Verteilen von Zugangsdaten (z. B. für ein gemeinsames Tauschlaufwerk) ist über diesen Weg möglich, da diese in der CFG-Datei nicht im Klartext gespeichert werden.
- **Variante 2** (JSON-Datei): Die Variante eignet sich zum Verteilen von Netzlaufwerken, bei denen lediglich der Pfad vorgegeben werden soll. Die Eingabe der Zugangsdatern erfolgt manuell durch die Lehrkraft. Die JSON-Datei lässt sich nach unten angegebenem Schema selbst erstellen und enthält u.a. die Informationen über den Netzwerkpfad, den Laufwerksbuchstaben und den Benutzernamen. Kennwörter können bei dieser Variante nicht mitüberegeben werden.

18.1 Variante 1: Verteilung eine CFG-Datei

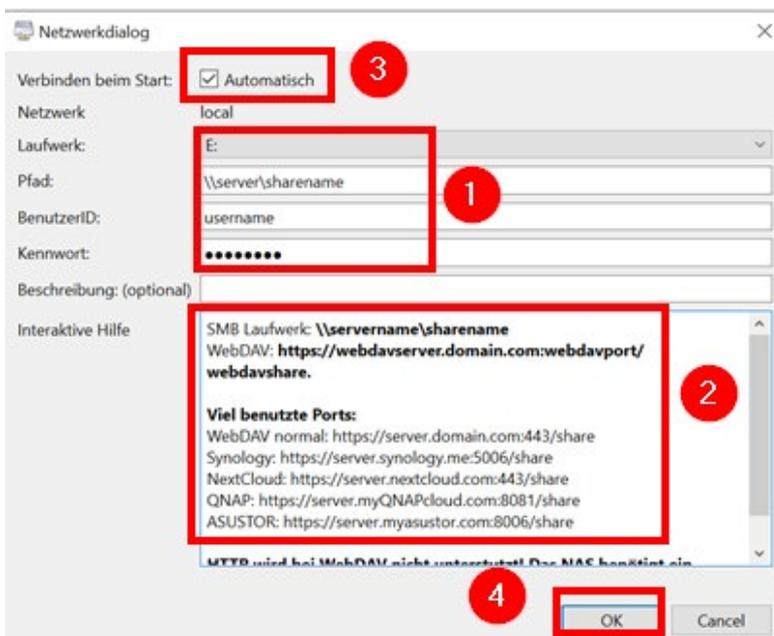
Zunächst auf einem Endgerät (z. B. einem Testgerät) die Software „MyDriveControl“ installieren. Die Software kann über den internen Appstore bzw. alternativ über <https://lubby.org/de/Software/MyDriveControl> heruntergeladen werden.

Die Software starten und „Netz hinzufügen“ wählen:





Laufwerksbuchstaben, Netzwerkpfad, Benutzername und Kennwort für das zu verteilende Netzlaufwerk eingeben (1), dazu die Hinweise zum Pfad beachten (2), bei Bedarf die automatische Verbindung beim Start aktivieren (3) und mit „OK“ bestätigen (4):



Ggf. weitere Netzlaufwerke anlegen.

Im Anschluss über „Schließen“ (1) und „Save“ (2) die Konfiguration abspeichern:

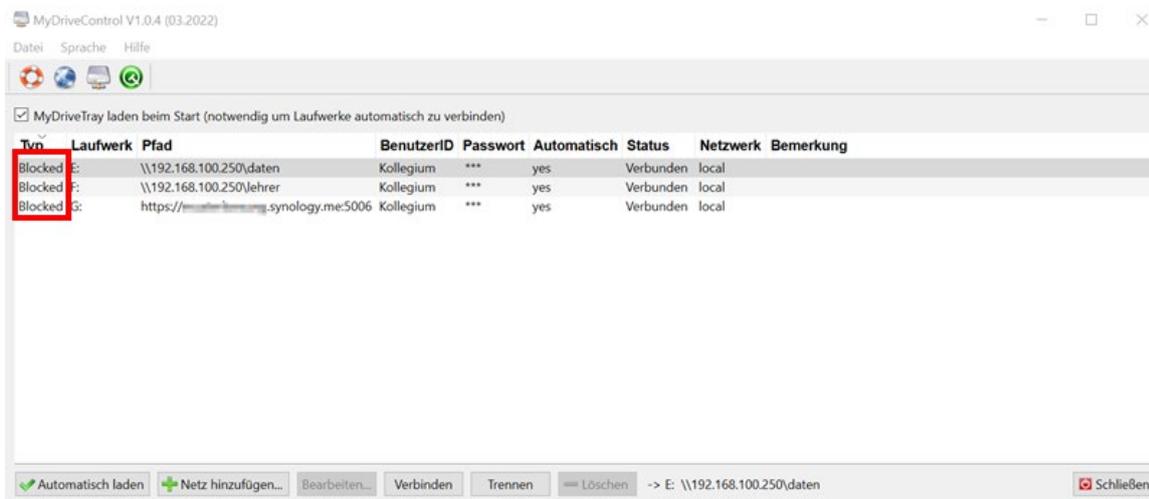


Im Ordner %localappdata%\Lubby\MyDriveControl befindet sich nun die Konfigurationsdatei „MyDriveControl.cfg“, die zur Verteilung der Netzlaufwerke über das UEM benötigt wird.

Die CFG-Datei über das UEM in den Zielpfad C:\Program Files\Lubby\MyDriveControl auf den Endgeräten kopieren (siehe Kapitel [Windows: Kopieren von Dateien/Ordern](#)).

Hinweis: Die CFG-Datei wird wie angegeben in den Programmpfad kopiert und nicht in den Ordner unter %localappdata%, damit das Abändern des Pfades durch die Lehrkraft über die Software „MyDriveControl“ gesperrt ist.

Nach einem (Neu-)Start der Software „MyDriveControl“ auf den Endgeräten werden die verteilten Laufwerke mit dem Typ „Blocked“ angezeigt:



Hinweis: Automatisch zu verbindende Laufwerke werden beim nächsten Gerätereustart eingebunden.

18.2 Variante 2: Verteilung einer JSON-Datei

Zunächst mit Hilfe eines Texteditors nach folgendem Schema die zu verteilenden Netzwerkpfade festlegen:

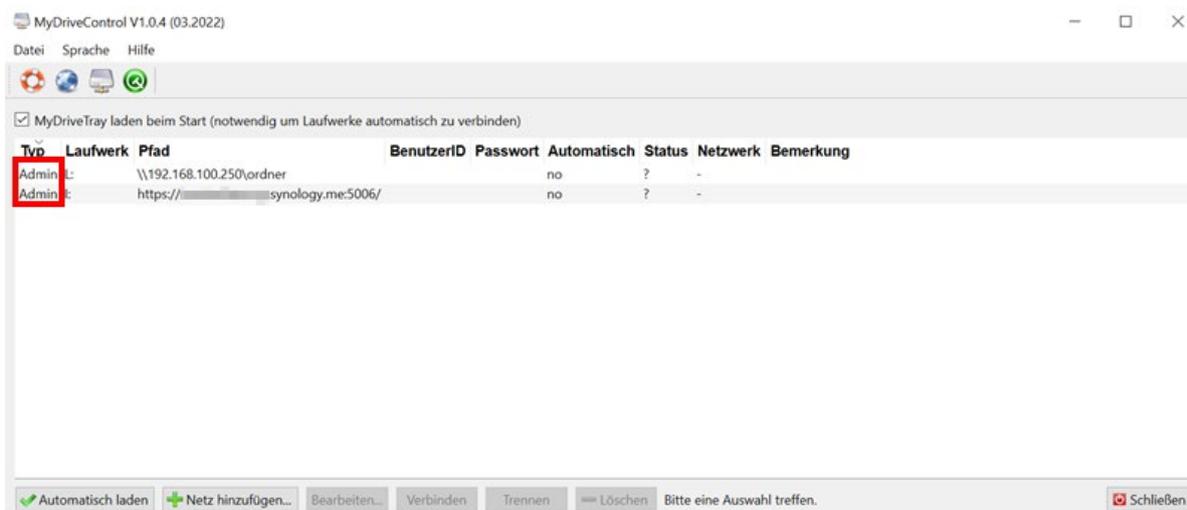
```
{ "Drives":
[
{
  "Type": "Admin",
  "Drive": "L:",
  "Path": "\\192.168.1.250\tauschordner",
  "UserID": "lehrer",
  "Comment": "SMB-Tauschordner Lehrkraefte"
},
{
  "Type": "Admin",
  "Drive": "M:",
  "Path": "https://gs-musterstadt.synology.me:5006/tauschordner",
  "UserID": "Benutzer",
  "Comment": "WebDAV-Tauschordner Lehrkraefte"
}
]
}
```

Hinweis: Mit dem Typ „Admin“ gekennzeichnete Laufwerke können durch die jeweilige Lehrkraft innerhalb der Software MyDriveControl gelöscht werden. Sie werden jedoch nach einem Neustart der Software automatisch wiederhergestellt. Benutzernamen können optional mitangegeben werden. Die Übermittlung von Kennwörtern ist auf diesem Wege nicht möglich.

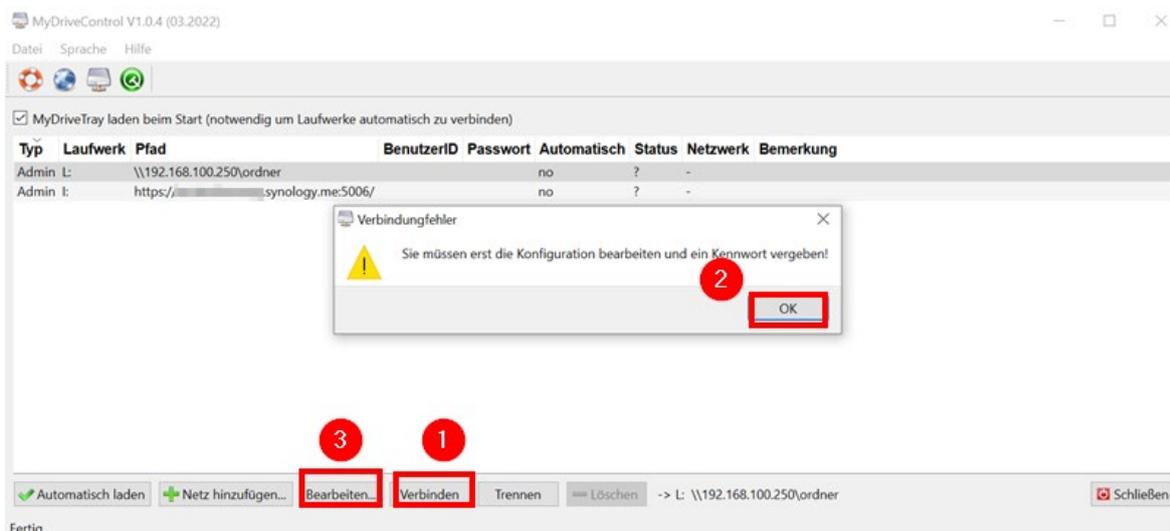
Die Datei als Datei mit dem Namen „MyDriveControl.json“ abspeichern.

Diese Datei über das UEM in den Zielpfad C:\Program Files\Lubby\MyDriveControl auf den Endgeräten kopieren (siehe Kapitel [Windows: Kopieren von Dateien/Ordern](#)).

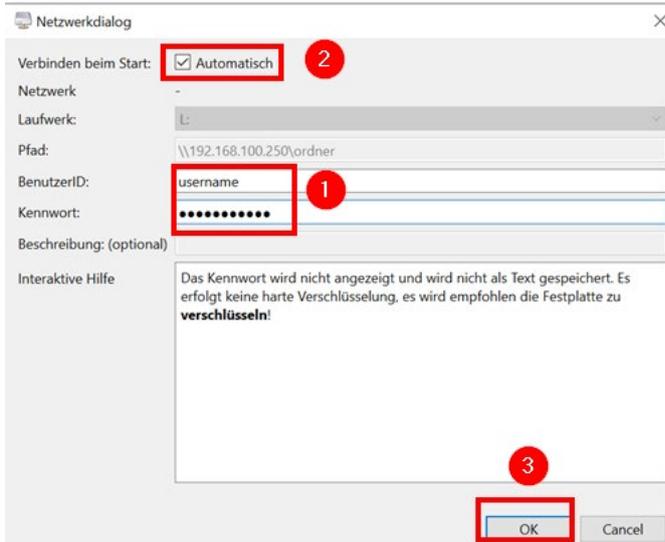
Nach einem (Neu-)Start der Software „MyDriveControl“ auf den Endgeräten werden die verteilten Laufwerke mit dem Typ „Admin“ angezeigt:



Versuchen Lehrkräfte über „Verbinden“ (1) die Laufwerke zu aktivieren, erscheint der Hinweis, dass zunächst die Zugangsdaten eingegeben werden müssen. Dazu muss die jeweilige Lehrkraft den Hinweis schließen (2) und „Bearbeiten“ (3) wählen:



Im Anschluss müssen die Zugangsdaten (1) eingegeben, ggf. die automatische Einbindung beim Start aktiviert (2) und mit „OK“ (3) bestätigt werden:



Hinweis: Soll ein Gastlaufwerk mit passwortfreiem Zugang eingerichtet werden, so muss auf dem Endgerät zunächst eine Gruppenrichtlinie aktiviert werden. Dazu im Suchfeld der Taskleiste „gpedit.msc“ eingeben und die Richtlinie „Computerkonfiguration“ – „Administrative Vorlagen“ – „Netzwerk“ – „LanMan-Arbeitsstation“ – „Unsichere Gastanmeldungen aktivieren“ auf „Aktiviert“ umstellen. Für MyDriveControl muss als BenutzerID ein beliebiger noch nicht vergebener Name (z. B. „gast“) verwendet werden. Zudem muss – auch wenn für den Gastzugriff kein Passwort benötigt wird – eine beliebige Kennung (z.B. „kennung“) angegeben werden.

19 Windows: Skripte verteilen

Das Kapitel beschreibt die Bereitstellung von Windows-Anwendungen und -Einstellungen mit Hilfe von Skripten.

19.1 Nutzungsszenarien von Skripten

Skripte können u. a. angewendet werden für folgende Szenarien:

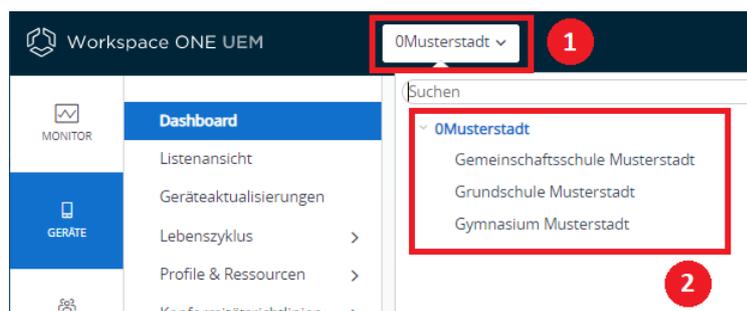
- Einträge in der Registry setzen
- Drucker installieren
- Netzlaufwerke einbinden (alternativ zur Methode im vorigen Kapitel)
- Installation großer Software-Pakete von lokalen Servern/NAS

19.2 Vorbereitung

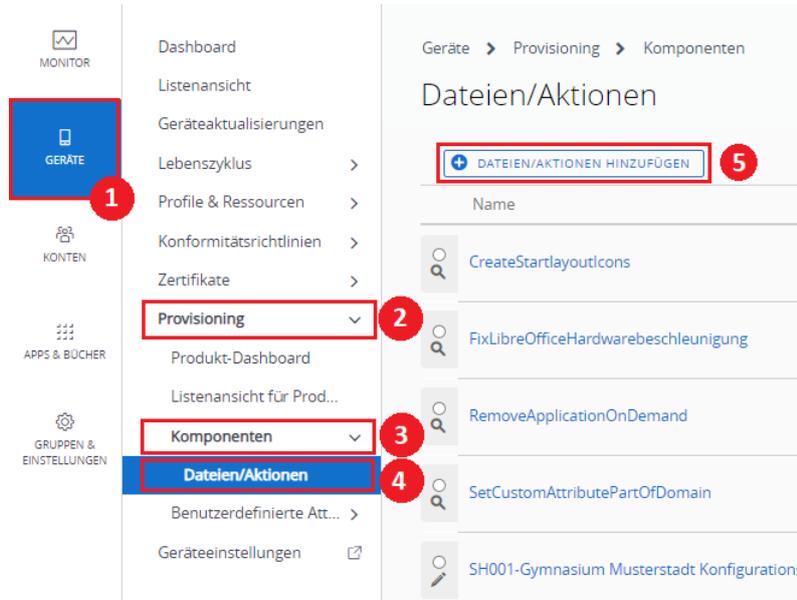
- Bereiten Sie das auszuführende Skript vor.
- Identifizieren Sie die Zuweisungsgruppe (Smartgroup) bzw. legen Sie ggf. eine geeignete Zuweisungsgruppe an.

19.3 Skript (Datei) anlegen

Prüfen Sie zunächst die Einstellung der Organisationsgruppe (Schul- oder Schulträger-Ebene).



Wechseln Sie anschließend in den Bereich „Geräte“ (1) – „Provisioning“ (2) – „Komponenten“ (3) – „Dateien/Aktionen“ (4), um das Skript als Komponente anzulegen. Klicken Sie dazu auf „Dateien und Aktionen hinzufügen“ (5).



Wählen Sie im erscheinenden Auswahlnenü die Plattform „Windows“:



Wählen Sie anschließend den Gerätetyp „Windows Desktop“:



In der sich anschließend öffnenden Maske vergeben Sie unter „Allgemein“ (1) einen Namen (2) entsprechend der Namenskonvention, der es Ihnen erlaubt, das Skript später eindeutig zu identifizieren.

GroupID (SH001)- -Schulname Skriptname

Bsp: SH001-0Musterstadt MeinSkript

Ergänzen Sie eine Kurzbeschreibung der Funktion (3) und ändern Sie bei Bedarf die zugehörige Organisationsgruppe (4).

Dateien/Aktionen hinzufügen

Allgemein Dateien Manifest

1

Name * SH001-0Musterstadt VPN-Attribut hinzufügen 2

Beschreibung Ergänzt Windows Registry Attribut 3

Version 1 ⓘ

Plattform Windows Desktop

Verwaltet von * 0Musterstadt 4

Wechseln Sie anschließend in den Bereich Dateien (1) und beginnen Sie den Upload des Skriptes über „Dateien hinzufügen“ (2).

Dateien/Aktionen hinzufügen

Allgemein **Dateien** Manifest

1

2

+ DATEIEN HINZUFÜGEN

Dateiname	Pfad	Version	Typ	Aktionen
Keine Datensätze gefunden.				

Wählen Sie im sich öffnenden Fenster das Skript über „Datei auswählen“ (1) und laden Sie diese mittels „Speichern“ (2) in das UEM hoch.

Dateien hinzufügen

Datei hinzufügen* **Dateien auswählen** 1

2 **SPEICHERN** ABBRECHEN

Definieren Sie Ziellaufwerk (1) und Version (2) des Skriptes und sichern Sie diese Informationen mittels „Speichern“ (3).

Dateien hinzufügen

Datei - 1

Name WIP_rfgg_vpn1.bat

Downloadpfad * C:\Windows 1

Version * 1.0 2

3 **SPEICHERN** ABBRECHEN

Wechseln Sie anschließend in den Bereich „Manifest“ (1) und fügen Sie über „Auszuführende Aktion“ (2) eine Operation hinzu, die auf das Skript angewendet werden soll.

Dateien/Aktionen hinzufügen



Wählen Sie anschließend die „Auszuführende Aktion(en)“ (1). Je nach ausgewählter Aktion werden weitere Eingabefelder aktiviert. Für Skripte empfiehlt sich die Aktion „Ausführen“. Dafür sind die Informationen „Kontext“ (2), „Befehlszeile und Argumente zur Ausführung“ (3) und ein Zeitlimit (5) erforderlich. Das von Dataport empfohlene Zeitlimit beträgt 5. Bestätigen Sie die Angaben durch „Speichern“.

Manifest hinzufügen

Auszuführende Aktion(en) * 1

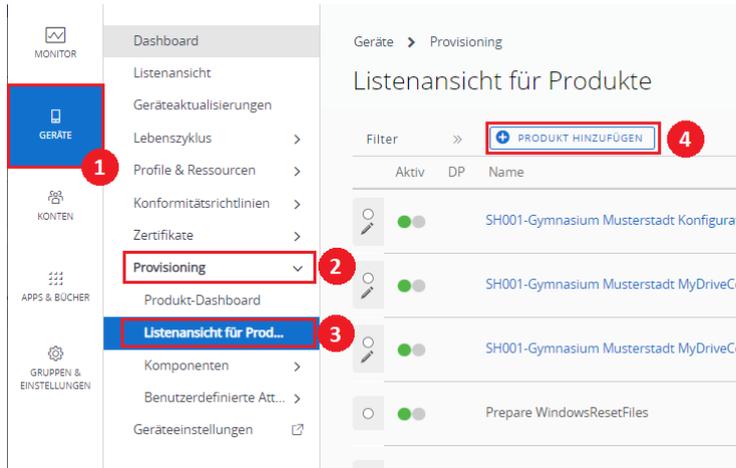
Ausführungskontext * 2

Befehlszeile und Argumente zur Ausführung * 3

Zeitlimit (-1 für unendlich) * 4

19.4 Produkt anlegen und aktivieren

Um eine Komponente einer Gruppe von Endgeräten zuweisen zu können, muss diese in ein Produkt eingebunden werden. Wechseln Sie im Bereich „Geräte“ (1) und dort im Untermenü „Provisioning“ (2) in die „Listenansicht der Produkte“ (3). Legen Sie ein neues Produkt über „Produkt hinzufügen“ (4) an.



Im Bereich „Allgemein“ (1) vergeben Sie einen Namen (2) entsprechend der Namenskonvention

GroupID -Schulname Produktname

Bsp: SH001-Musterstadt MeinProdukt

Ergänzen Sie eine Kurzbeschreibung (3), prüfen Sie die Organisationseinheit (4) und weisen Sie eine oder mehrere Zuweisungsgruppen/Smartgroups (5) zu.

Produkt hinzufügen

Fügen Sie über Manifest (1) eine auszuführende Aktion hinzu (2).

Produkt hinzufügen



Ändern Sie die „Auszuführende Aktion“ auf „Datei/Aktion installieren“ (1) und wählen Sie die zuvor angelegte Datei (Komponente) (2).

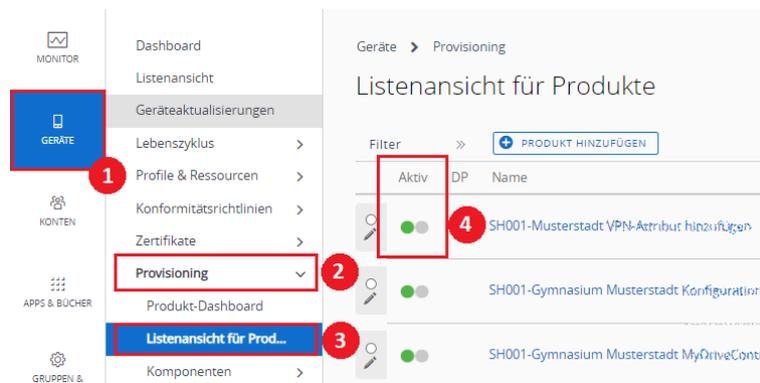
Manifest hinzufügen



„Speichern“ (2) Sie Ihre Einstellungen und „Aktivieren“ (3) Sie das Produkt für die Bereitstellung. Die Aktivierung kann ggf. auch zu einem späteren Zeitpunkt erfolgen.



Prüfen Sie den gewünschten Status (4) in der „Listenansicht der Produkte“ (3) im Bereich „Provisioning“ (2).



Über das Stiftsymbol unterhalb des Radio-Buttons lassen sich die Einstellungen des Produktes bei Bedarf bearbeiten.

20 Änderungshistorie

Änderung in Handbuch-Version 2.9:

- Anleitung zum [Passwort zurücksetzen und Gerät zurücksetzen](#) für Windows Endgeräte aktualisiert

Änderung in Handbuch-Version 2.8:

- Anleitung zum [App-Konfiguration verteilen](#) für iPads hinzugefügt

Änderung in Handbuch-Version 2.7.1:

- Hinweise zum Einbinden von Windows-Testgeräten und zum Löschen von Windows-Paketen ergänzt

Änderung in Handbuch-Version 2.7:

- Die Schritte zur Installation weiterer Schriften auf iPads wurden hinzugefügt. (siehe Kapitel [iPadOS: Schriftarten hinzufügen](#))

Die Anlage von Nutzungsbedingungen wurden hinzugefügt. (siehe Kapitel [Anlegen von Nutzungsbedingungen](#))

Änderung in Handbuch-Version 2.6:

- Die Schritte zur Verwendung von Skripten zur Administration von Windows-Endgeräten (siehe Kapitel [Windows: Skripte verteilen](#)) wurden hinzugefügt.

Änderung in Handbuch-Version 2.5:

- Die Schritte zur Zurücksetzung des Geräte-Passwortes für iPads (siehe Kapitel [iPadOS: Kennung zurücksetzen](#)) und für Windows (siehe Kapitel [Windows: Passwort zurücksetzen](#)) wurden hinzugefügt.

Änderung in Handbuch-Version 2.4:

- Die Schritte zur Paketerstellung für eine App aus dem Microsoft Store wurden hinzugefügt (siehe Kapitel [Paketierung Microsoft-Store-App](#)).

Änderungen in Handbuch-Version 2.3:

- Die Schritte zum Zurücksetzen des Passwortes für den UEM-Account des Basic-Benutzers wurden hinzugefügt (siehe Kapitel [Basic-Benutzer: Passwort zurücksetzen](#)).
- Ein Kapitel zur Verteilung von Netzlaufwerken für Windows-Endgeräte wurde hinzugefügt (siehe Kapitel [Windows: Netzlaufwerk verteilen](#)).

Änderung in Handbuch-Version 2.2:

- Die Schritte zum Kopieren einer Lizenzdatei für die Anwendung Worksheetcrafter wurde ergänzt (Kapitel 11.5.1).

Änderung in Handbuch-Version 2.1:

- Die Schritte zum Kopieren einer Lizenzdatei für bestimmte Anwendungen (ActivInspire, Budenberg, Lernwerkstatt) über das UEM wurden ergänzt (Kapitel 11.5.1).
- Die Schritte zur Paketerstellung für Microsoft Office 2016 wurden ergänzt (Kapitel 11.6.1).

Änderung in Handbuch-Version 2.0:

- Die Schritte zur Einbindung von Test-iPads wurden ergänzt (Kapitel 4.2).

Änderung in Handbuch-Version 1.2:

- Das Kapitel [Microsoft Office-Paketierung](#) wurde hinzugefügt.