MS365 Verwaltungstool

für die Geräte der Geräteinitiative

Vorarlberger Bildungsservice
Verfasser: Martin Schnetzer
Besuchen Sie uns im Internet
http://www.vobs.at/rb

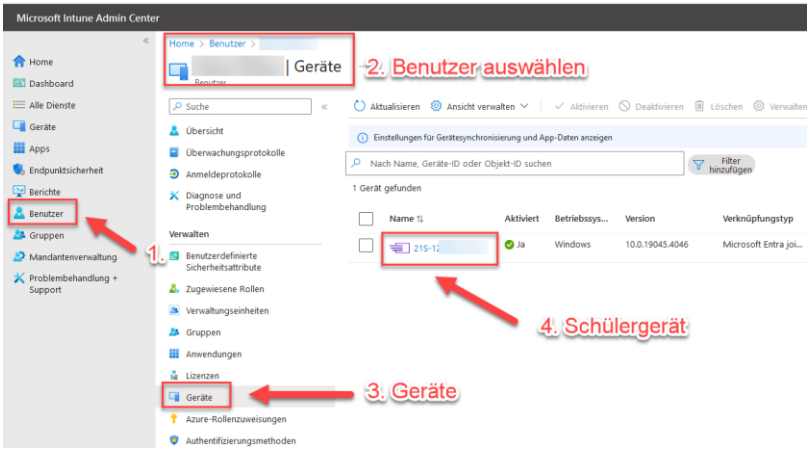
1. Inhaltsverzeichnis

2. Vorbemerkungen

Das MS365 – Verwaltungstool wurde vorrangig für die Geräte der Geräteinitiative des Bundes programmiert, um diese aus der Microsoft365 Intune Verwaltung zu löschen.

Das Programm kann unter https://download.vobs.at heruntergeladen werden. Sollte kein Zugang zum Download-Bereich vorhanden sein, melden Sie sich bitte unter schnetzer@vobs.at.
Video-Tutorials sind unter https://screencast.vobs.at zu finden.

Damit das Programm ordnungsgemäß funktioniert, muss bei den Schüler:innen das betreffende Gerät hinterlegt sein. Kontrolliert wird das im Intune Admin Portal (https://intune.microsoft.com).



Bei diesem Schüler ist ein Windows Autopilot bzw. iPad Gerät registriert, welches mit dem MS365 Verwaltungstool komplett gelöscht wird.

Erklärung Windows Geräte – offboarding:
Windows Autopilot Geräte können nicht einfach aus Intune gelöscht werden. Es muss zuerst das Autopilot-Profil gelöscht werden. Im Anschluss kann das Gerät vom Benutzer getrennt werden. Nachdem das Gerät gelöscht wurde, wird auf dem betreffenden Gerät das Arbeitsprofil gelöscht. Nach dem Löschen des Profils kann nur noch mit einem lokalen Administrator auf das Gerät zugegriffen werden.

Erklärung iPad Geräte – offboarding:
iPad Geräte müssen in zwei verschiedenen Portalen gelöscht werden. Dabei spielt die Reihenfolge eine wichtige Rolle. Löschen der Geräte im ASM (Apple School Manager) anschließend im Intune. Beim letzten Schritt werden die iPads zurückgesetzt und eine private Apple-ID ist erforderlich.

Das MS365 – Verwaltungstool basiert auf Microsoft PowerShell. Ein Ausführen des Programmes ist auf Microsoft - Windows® Rechner begrenzt. Damit das Programm ordnungsgemäß funktioniert, müssen folgende Punkte beachtet werden.

2.1. Welche Administratorrolle ist notwendig?

Für die einzelnen Bereiche des MS365-Verwaltungstools sind z.T. unterschiedliche Berechtigungen notwendig. Um das Programm ausführen zu können muss der Benutzer ein **globaler Administrator** oder ein **Intune-Administrator mit** der zusätzlichen Rolle **Cloud-Anwendungsadministrator** sein. Der **Cloud-Anwendungsadministrator ist bei nicht globalen Admins zwingend erforderlich**.

	Globaler Administrator	Cloud-Anwendungsadministrator	Intune-Administrator	Teams-Administrator
Bitlokcer Key	X	X	X	
Windows Geräte	X	X	X	
iPad Geräte	X	X	X	
Veyon Klassenliste	X	X	x	
Teams	X	X		x

2.2. Vorgehensweise Offboarding von iPads und Windows Tablets

Grundsätzlich sollte pro Klasse eine Doppelstunde Digitale Grundbildung in der vorletzten/letzten Schulwoche eingeplant werden. Weiters sollte an diesem Tag der MDM-Verantwortliche zusätzlich zur Verfügung stehen. Der MDM-Verantwortliche löscht Klassenweise/Schulweise die Geräte von den betreffenden Schüler:innen.

Was geschieht, wenn die Geräte gelöscht wurden?

iPad Geräte:
Beim Löschen der iPad Geräte wird das Gerät auf die Werkseinstellungen (alle Apps – auch Office – werden gelöscht) zurückgesetzt. Es werden alle Daten und Einstellungen vom iPad gelöscht und können nicht wiederhergestellt werden. Im Vorfeld ist mit den Schüler:innen zu besprechen, wie sie auf die in der Cloud gespeicherten Daten zugreifen können. Dafür werden die Microsoft Zugangsdaten benötigt. Das Schulkonto (inkl. aller Daten) werden vom verantwortlichen IT-Kustoden der Schule im Herbst unwiderruflich gelöscht. Ab diesem Zeitpunkt kann nicht mehr auf die in Onedrive gespeicherten Daten, E-Mails, etc. zugriffen werden. Die Lizenzierung von Office erlischt.

Windows Geräte:
Beim Löschen der Windows Geräte wird das Schüler-Profil (Unternehmenskonto) auf dem Gerät entfernt. Damit werden alle von der Schule bereitgestellten Programme gelöscht (Ausnahme Win32 Pakete). Nach dem Entfernen des Profils ist ein Login nur noch über den lokalen Benutzer/Administrator möglich. Dieser muss mit den Schüler:innen im Vorfeld nochmals kontrolliert bzw. einen lokalen Benutzer für das tägliche Arbeiten erstellt werden. Weiters ist im Vorfeld mit den Schüler:innen zu besprechen, wie sie auf die in der Cloud gespeicherten Daten zugreifen können. Dafür werden die Microsoft Zugangsdaten benötigt. Das Schulkonto (inkl. aller Daten) werden vom verantwortlichen IT-Kustoden der Schule im Herbst unwiderruflich gelöscht. Ab diesem Zeitpunkt kann nicht mehr auf die in Onedrive gespeicherten Daten, E-Mails, etc. zugriffen werden. Die Lizenzierung von Office erlischt.

Sollte auf dem Windows Tablet eine Bitlocker-Verschlüsselung aktiviert sein, muss diese im Vorfeld mit dem MS365-Verwaltungstool ausgelesen werden. Der Gerätebezogene Key kann im Anschluss mit einem Serienbrief den Schüler:innen ausgeteilt werden.

Achtung: Nach dem Löschen des Gerätes steht der Bitlocker-Key nicht mehr zur Verfügung. Ohne Bitlocker-Key kann das Gerät nur noch neu installiert werden, dabei gehen alle auf dem Gerät gespeicherten Daten und Einstellungen verloren.

2.3. PowerShell Kontrolle

- Microsoft.Graph muss in einer aktuelleren Version installiert sein, **Minimumversion 2.6.12**.

Eine Installation bzw. ein Update von Microsoft Graph erfolgt in einer **Administrativen PowerShell-Konsole**. Dazu sind Administratorenrechte auf dem Computer notwendig.

Um PowerShell Scripte installieren zu können, muss zuerst die **Execution-Policy** geändert werden.

Vorgehensweise der Installation von Microsoft Graph:
- Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
- Install-Module microsoft.graph -Repository PSGallery -Force

Update des Moduls Microsoft Graph
- update-module microsoft.graph

Video-Tutorial auf https://screencast.vobs.at

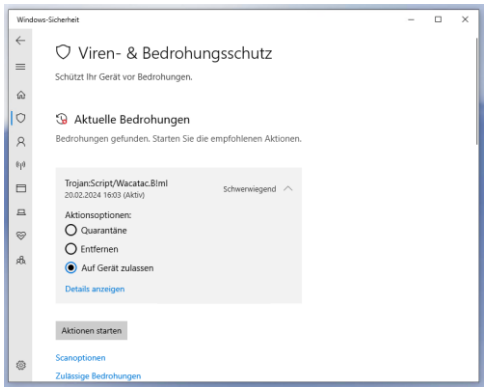
2.4. Nutzung des Programms

Das Programm kann nur von einem bestimmten Benutzer (siehe 2.1) verwendet werden.

Mögliche Probleme:

F: Antivirenprogramm erkennt das Programm als Virus an. Programm wird sofort gelöscht.
A: Das Programm als Vertrauenswürdig markieren und zulassen

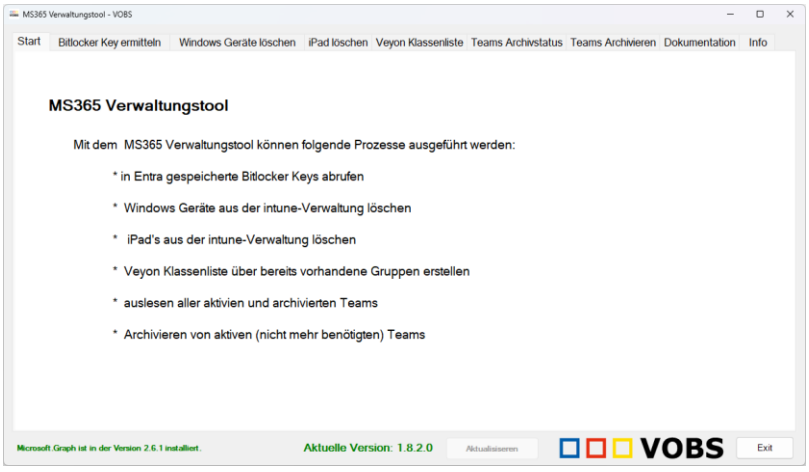
Im Viren- & Bedrohungsschutz den passenden Eintrag ändern und das Programm ist ausführbar. Das Problem liegt in der Erstellung der EXE-Datei – ES IST KEIN VIRUS 😊



F: MS365 – Verwaltungstool verbindet sich nicht mit dem Tenant.
A: Microsoft.Graph ist nicht in der richtigen Version installiert (zu alte Version → siehe Update Microsoft.Graph)

3. Programmaufbau

Der Programmstart des MS365-Verwaltungstool dauert ein wenig. Während des Startens werden diverse Ordner angelegt, eine Versionsüberprüfung durchgeführt und kontrolliert ob und in welcher Version Microsoft Graph installiert ist.



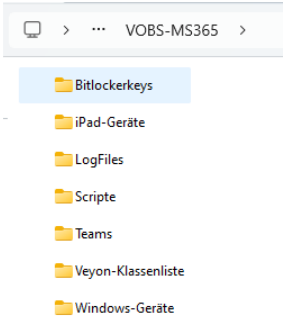
Beim Klicken auf die Register wird die Verbindung zum Tenant jeweils beendet. Die verschiedenen Prozesse benötigen verschiedene Anmelderegeln und Berechtigungen.

In der unteren Zeile ist erkennbar, ob die installierte Graph-Version ausreichend ist. Auch eine Verfügbarkeit eines Updates wird angezeigt.

Update/Aktualisieren:
Ist eine neue Version online verfügbar, wird sie direkt angezeigt. Die Aktualisierung erfolgt über die Schaltfläche „Aktualisieren“. Dabei schließt sich das Hauptfenster und das Verwaltungstool erstellt im Lokalen Arbeitsverzeichnis C:\VOBS-MS365\Backup ein ZIP-komprimiertes Backup mit allen im Verzeichnis VOBS-MS365 vorhandenen Dateien. Dieses kann bei Bedarf wieder extrahiert werden.

Startvorgang des MS365-Verwaltungstool:
Wie bereits erwähnt, werden verschiedene Prozesse vor dem Programmstart abgearbeitet.

Folgende Ordner werden im Ordner auf C:\VOBS-MS365\ angelegt. Zusätzlich wird eine Vorlagen-Userlisten im Ordner iPad-Geräte und im Ordner Windows-Geräte angelegt: Die Userlisten enthalten nur die Überschrift. Diese darf nicht gelöscht werden.



4. Bitlocker

BitLocker ist eine proprietäre Festplattenverschlüsselung von Microsoft, die zu den Features von Windows gehört. Es handelt sich um eine Sicherheitsfunktion, die in bestimmten Versionen des Windows-Betriebssystems integriert ist. Die Hauptaufgabe von BitLocker besteht darin, Daten auf Systemlaufwerken, Festplatten oder Wechseldatenträgern zu verschlüsseln. Dadurch werden die gespeicherten Daten gegen Diebstahl und unbefugtes Lesen geschützt. Wenn du BitLocker aktivierst, verwendet es standardmäßig den AES-Verschlüsselungsalgorithmus im Cipher Block Chaining (CBC)- oder XTS-Modus mit einer Schlüssellänge von 128 oder 256 Bit.

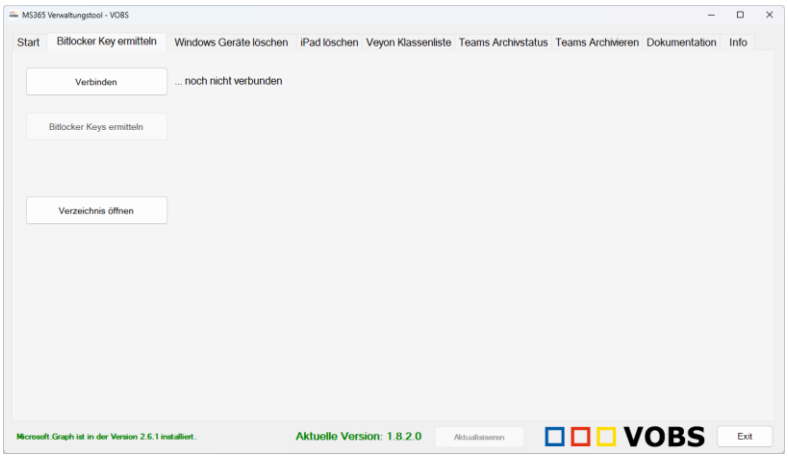
Die Vorteile von BitLocker sind:

- Datenschutz: BitLocker schützt deine persönlichen Daten vor fremdem Zugriff, falls dein Gerät gestohlen wird oder verloren geht.
- Verschlüsselung: Es verschlüsselt die gesamte Festplatte, wodurch die Daten sicher sind, selbst wenn jemand physischen Zugriff auf das Laufwerk hat.
- Einfache Aktivierung: BitLocker ist bereits bei aktuellen Geräten mit TPM (Trusted Platform Module) von Werk aus aktiviert.

Es ist wichtig zu beachten, dass BitLocker nicht vor Angriffen aus dem Internet schützt. Wenn dein Rechner defekt ist, kann es jedoch schwierig sein, die Daten auszulesen, selbst wenn sie unverschlüsselt sind.

Ist der BitLocker aktiviert, so werden die Keys automatisch im Entra Admin Center gespeichert. Ein Auslesen des Wiederherstellungsschlüssels ist nur einzeln über die grafische Oberfläche möglich.

4.1. Auslesen des BitLocker Wiederherstellungsschlüssels



Verbinden mit dem MS365 Tenant als Administrator – siehe 2.1 – (beim erstmaligen Verbinden muss die Nutzung des Graphen erlaubt werden – siehe Screenshot 1 im Anhang)

Nach erfolgreicher Verbindung ist der Name der Schule ersichtlich.

Bitlocker Keys ermitteln – dieser Schritt dauert ein paar Sekunden. Es werden nun alle im Tenant registrierten Geräte abgefragt.

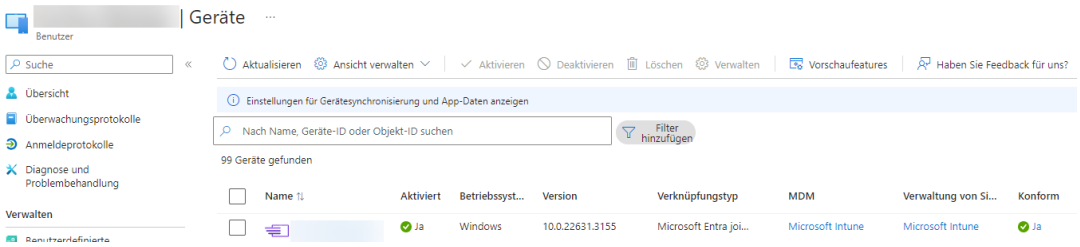
Beim Klicken auf „Verzeichnis öffnen“ ist nun die erstellte Bitlockerkey_Datum.csv ersichtlich. Diese kann nun entsprechend weiterverwendet werden.

Die BitLocker Widerherstellungsschlüssel können mit Hilfe eines Serienbriefes den Schüler:innen ausgeteilt werden.

Wurde ein Gerät aus der Verwaltung gelöscht, so kann der Wiederherstellungsschlüssel nicht mehr ausgelesen werden.

5. Windows Geräte löschen

Windows Autopilot Geräte benötigen einen zusätzlichen Schritt im Intune Admin Center. Diese Geräte können nicht direkt beim User gelöscht werden. Ein Autopilot Gerät erkennt man am folgenden Symbol:



Zuerst müssen die Autopilot-Profile gelöscht werden, erst danach ist es möglich die Geräte zu löschen. Beim Löschen der Autopilot-Profile passiert User-seitig nichts. Merkbar wäre es nur dann, wenn das Gerät neu installiert wird. Nach dem löschen des Autopilot-Profils, ändert sich das Symbol beim jeweiligen Computer .

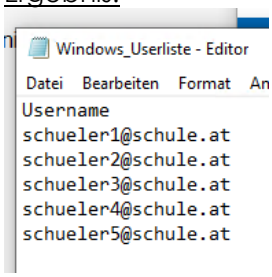
5.1. Löschen der Geräte

Die Geräte können nur gelöscht werden, wenn sie beim jeweiligen User (Schüler) registriert sind. Das Programm untersucht den User auf ein vorhandene(s) Gerät(e). Wird ein Autopilot Gerät gefunden so wird im ersten Schritt das Autopilot Profil entfernt. Dies dauert im Intune Admin Center mehrere Minuten, bis es korrekt angezeigt wird. Beim User ist es bereits sofort ersichtlich (siehe Symbol 5.).

Vorbereitung:
In der Datei Windows_Userliste.csv werden die Usernamen eingetragen, bei denen das Gerät gelöscht werden soll. Die Datei befindet sich im Ordner C:\VOBS-MS365\Windows-Geräte. Sie kann auch über die Schaltfläche „Verzeichnis öffnen“ bzw. „Durchsuchen“ geöffnet werden.

Achtung: Die Überschrift „Username“ darf nicht gelöscht werden!

Ergebnis:



Folgende Schritte müssen nun ausgeführt werden:

- Verbinden: verbinden mit einem geeigneten Administrator
- Durchsuchen: bereits erstellte Windows_Userliste.csv auswählen
- Autopilot Profil löschen: nun werden nur die Autopilot Profile gelöscht
- Geräte löschen: die Geräte werden gelöscht, ein Anmelden am Gerät ist nur noch mit einem lokalen Administrator möglich

Im Verzeichnis Windows-Geräte befinden sich nun zwei TXT-Dateien:

- Schule_Geloeschte_Windows_Autopilot_Profile_Datum.txt
- Schule_Geloeschte_Windows_Geraete_2024-02-20.txt“

Somit wurde das Gerät aus dem Microsoft 365 Tenant gelöscht. Ist das gelöschte Gerät mit dem Internet verbunden, werden alle Programme, welche per Intune verteilt wurde, gelöscht. Ausnahme sind Win32-Apps. Nach dem Neustart ist ein Anmelden nur noch mit einem lokalen Administrator möglich.

6. iPad Geräte löschen

Die Verwaltung der iPads ist in den Portalen Intune-Admin-Center und dem ASM (Apple School Manager) verortet.

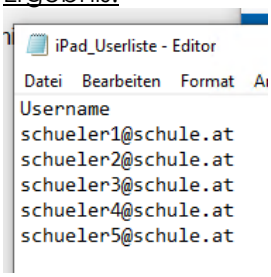
Da ein Entfernen von iPads ein zurücksetzen des Gerätes zur Folge hat, müssen sie zuerst aus dem ASM gelöscht werden. Es gibt keine PowerShell-Schnittstelle zum ASM, die das über eine Kommandozeile ermöglicht. Dennoch müssen die iPads nicht einzeln aus dem ASM gelöscht werden.

Nachdem die iPads aus dem ASM gelöscht wurden, werden sie im nächsten Schritt in Intune entfernt. Dabei wird ein Zurücksetzungsbefehl an das Gerät gesendet. Dieser wird ausgeführt, wenn sich das Gerät mit dem Internet verbindet.

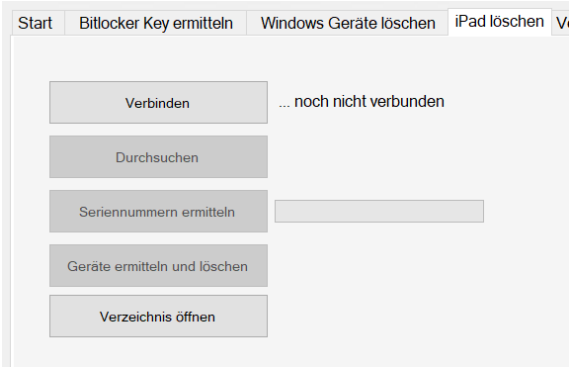
Vorbereitung:
In der Datei iPad_Userliste.csv werden die Usernamen eingetragen, bei denen das Gerät gelöscht werden soll. Die Datei befindet sich im Ordner C:\VOBS-MS365\iPad-. Sie kann auch über die Schaltfläche „Verzeichnis öffnen“ bzw. „Durchsuchen“ geöffnet werden.

Achtung: Die Überschrift „Username“ darf nicht gelöscht werden!

Ergebnis:

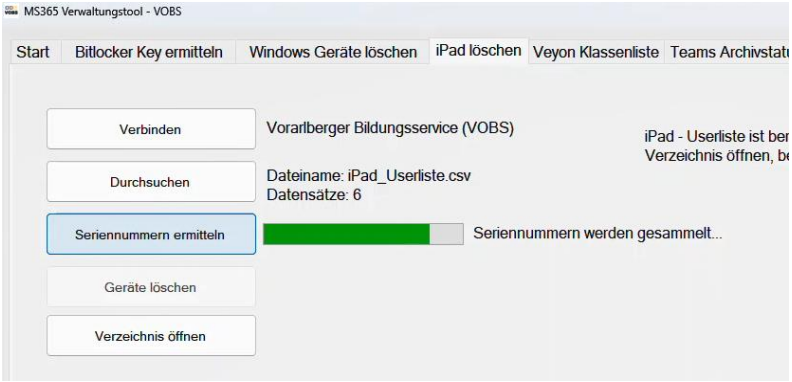


6.1. Löschen der Geräte

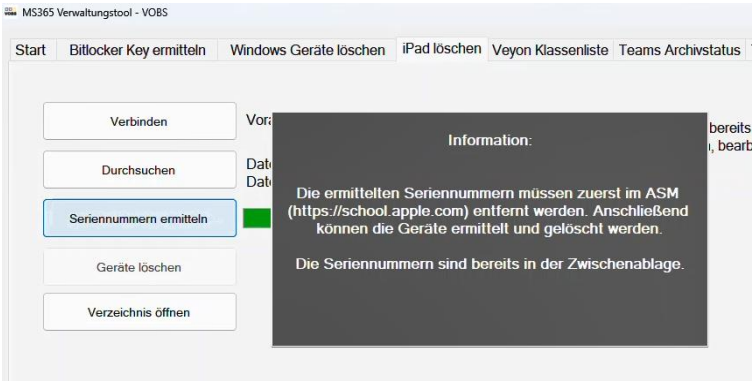


Folgende Schritte müssen nun ausgeführt werden:

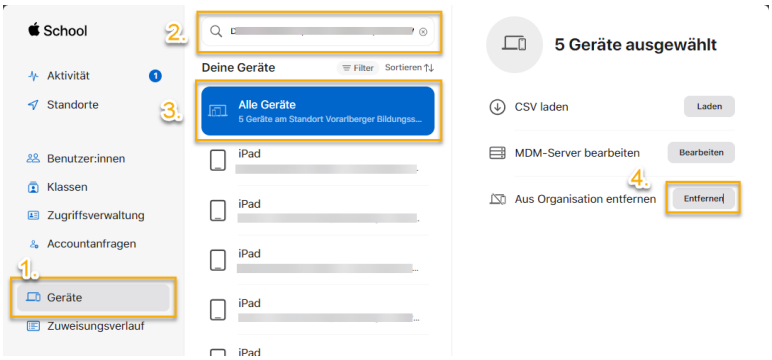
- Verbinden: verbinden mit einem geeigneten Administrator – siehe 2.1
- Durchsuchen: bereits erstellte iPad_Userliste.csv auswählen
- Seriennummern ermitteln: nun werden die Seriennummern gesammelt und in die Zwischenablage kopiert.
- Geräte ermitteln und löschen: die Geräte werden gelöscht und zurückgesetzt



Die Seriennummern werden in diesem Schritt ermitteln und in die Zwischenablage kopiert. Weiters wird auch eine TXT-Datei im Ordner iPad-Geräte erstellt, in welcher die ermittelten Seriennummern gespeichert werden (Schule_Seriennummern_Ipad_fuer_ASM_Datum.txt)



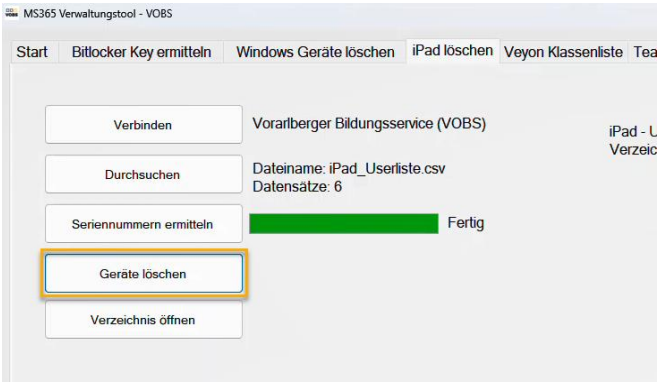
Im ASM müssen nun die Geräte gesucht und aus der Organisation gelöscht werden. Erst nach dem Löschen aus dem ASM kann das Gerät ohne MDM-Verwaltung installiert werden.



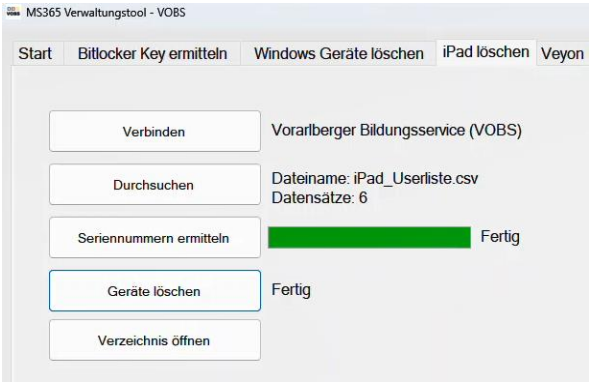
Befolge die Schritte 1-4:

1. Geräte
2. Seriennummern einfügen (befinden sich in der Zwischenablage)
3. Alle Geräte anklicken
4. Aus Organisation entfernen
5. Weiter geht es im MS365 Verwaltungstool

Im MS365-Verwaltungstool muss als letzter Schritt Geräte löschen geklickt werden.



Ergebnis:



Im Verzeichnis iPad-Geräte befinden sich nun zwei TXT-Dateien:

- Schule_Seriennummern_Ipad_fuer_ASM_Datum.txt
- Schule_Geloeschte_iPad_Geraete_Datum.txt

In der Seriennummern-Datei sind alle zu löschenden Seriennummern gespeichert (nur zur evtl. Kontrolle).

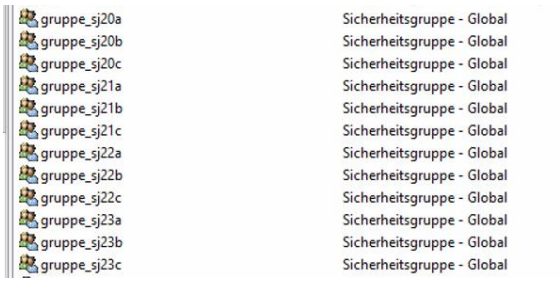
In der Gelöschte iPad Geräte Datei sind nun alle User mit ihrem Gerät aufgelistet. Sollte kein Gerät beim User notiert sein, so wurde beim betreffenden User nichts gefunden.

Das iPad wird, sofern es mit dem Internet verbunden ist, sofort zurückgesetzt. Es besteht keine Möglichkeit diesen Befehl zu widerrufen.

7. Veyon Klassenliste erstellen

Grundvoraussetzung:

Im lokalen ActiveDirectory müssen Sicherheitsgruppen vorhanden sein, in denen die Schüler:innen einer Klasse einer AD-Gruppe zugeordnet wurden. Die Nomenklatur der Gruppe spielt dabei keine Rolle. Wurde der TJ Usermanager verwendet, wurden die Schüler:innen bereits in Klassen angelegt. Wenn nicht vorhanden, kann eine zusätzliche Klassen AD-Gruppe erstellt werden

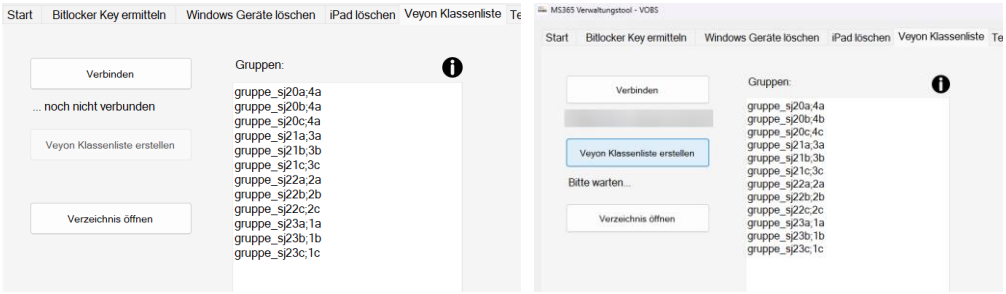


Der Gruppenname wird für das Erstellen der Veyon-Klassenlisten benötigt.

7.1. Veyon Klassenliste erstellen

In das Eingabefeld (Gruppen) werden nun die ActiveDirectory-Gruppen eingetragen, in denen die Schüler:innen der Klassen enthalten sind. Damit eine übersichtliche Klassenliste erstellt werden kann, wird der Gruppenname mit betreffenden Klasse ergänzt.

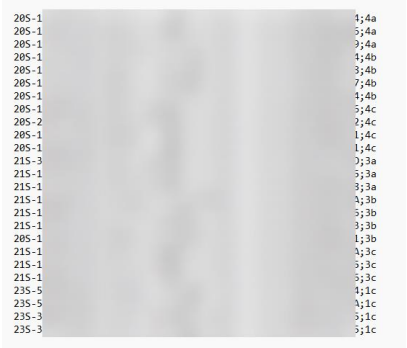
Beispiel: gruppe_sj21a;4a



Nach dem Verbinden wird nun die Klassenliste erstellt („Veyon Klassenliste erstellen). Nach erfolgreichem Auslesen, werden nun die Schüler:innen mit dem entsprechenden Gerät (aktuellen Gerätenamen), MAC-Adresse und dem Standort (Klasse) in die CSV-Datei **Schule_Klassenliste_Veyon_Datum.csv** exportiert.

Über die Schaltfläche „Verzeichnis öffnen“ kann diese gefunden werden.

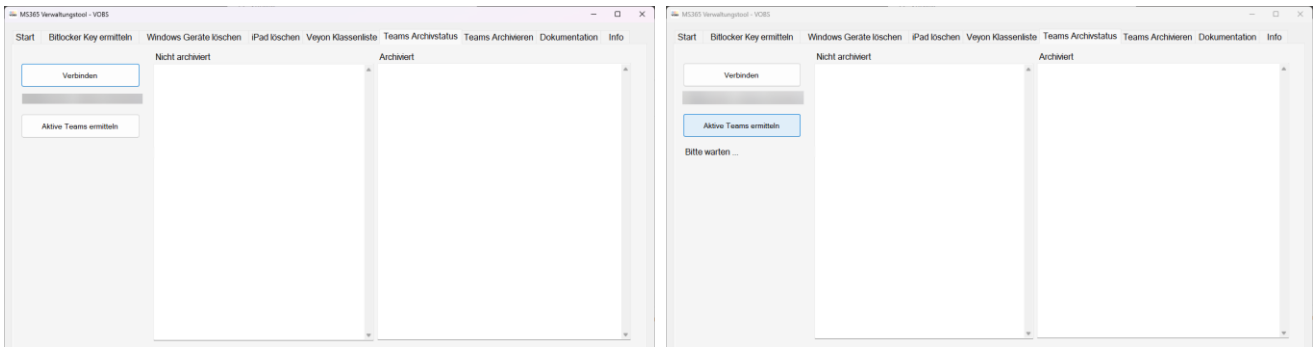
Ergebnis:



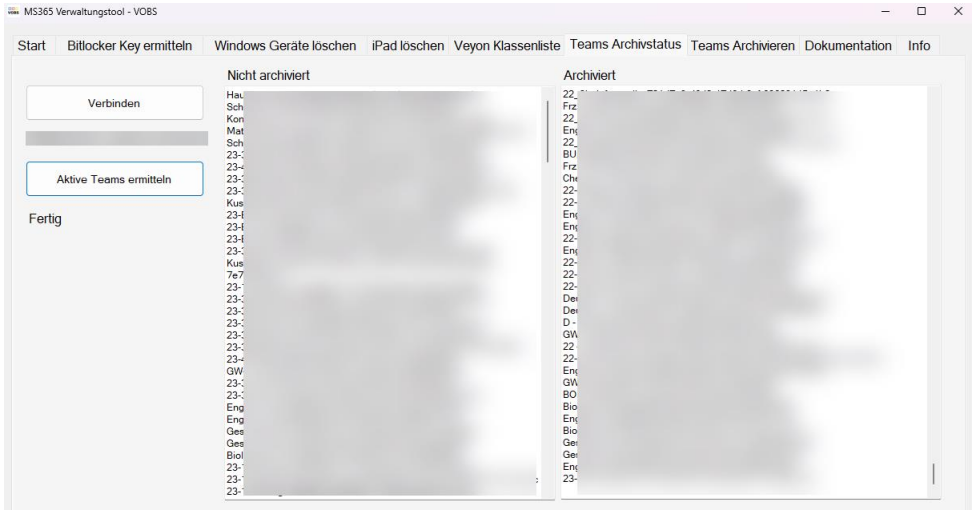
Achtung: Diese Klassenliste wird überschrieben, wenn sie am gleichen Tag noch einmal erstellt wird.

8. Teams Archivstatus

Unter dem Punkt Teams Archivstatus kann der Microsoft Tenant auf aktive und archivierte Teams untersucht werden. Werden nicht mehr benötigte Teams nicht archiviert, so scheinen sie beim Benutzer aktiv auf. Archivierte Teams können trotzdem durch den Benutzer geöffnet werden.



Nach dem Verbinden mit dem Tenant, werden die **Aktiven Teams ermittelt**. Es werden alle nicht archivierten und archivierten Teams angezeigt. Die angezeigten Teams dienen nur zur Information.



Im Verzeichnis Teams befinden sich nun zwei TXT-Dateien:

- Schule_Archivierte_Teams_Datum.csv
- Schule_Nicht_archivierte_Teams_Datum.csv

9. Teams Archivieren

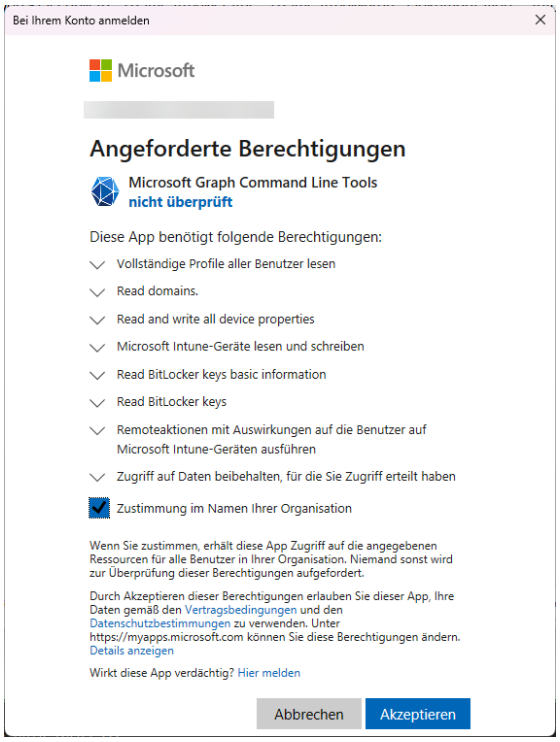
Für das Archivieren von einzelnen Teams ist die Team-ID notwendig, dies wurde im Kapitel 8 Teams Archivstatus ausgelesen.

Um nun einzelne Teams zu archivieren, werden nun die gefundenen Datensätze der nicht archivierten Teams in die TextBox kopiert. Dabei ist darauf zu achten, dass der komplette Zeileneintrag kopiert wird.

Beim Klicken auf die Schaltfläche „Teams archivieren“ werden die einzelnen Teams archiviert. Zur Kontrolle kann Kapitel 8 wiederholt werden.

Wurden versehentlich ein Team archiviert, so kann die Archivierung für jedes versehentlich archivierte Team im Teams Admin-Center (https://admin.teams.microsoft.com/teams/manage) rückgängig gemacht werden.

10. Anhang



Screenshot 1