

KINDERSCHUTZ 2026 MIT DEM CCCS - WINDOWS

Vorarlberger Standardschulinstallation
Verfasser: Martin Schnetzer

© 2026 IT-Regionalbetreuer Vorarlberg 6900
Bregenz, Römerstraße 14 Alle Rechte
vorbehalten

1 Warum überhaupt?

Das Ministerium hat in Zusammenarbeit mit mehreren MDM-Verantwortlichen einiger Bildungsdirektionen gemeinsame zentrale Richtlinien und Empfehlungen zum Kinderschutz bei den Geräten der Geräteinitiative ausgearbeitet.

 Die Einrichtung des Kinderschutzes ist ****obligatorisch****, die Verwendung der technischen Richtlinien optional - aber von unserer Seite aus empfohlen.

2 Grundsätzliche Funktionsweise

Ein Überblick über die Richtlinien ist auf den Webseiten des Ministeriums unter <https://bildungsministerium.atlassian.net/wiki/external/M2QyMmNiZTEzYTQ0NDZmYjgwYjY4ODU5YzU2MDcwYmU> abrufbar.

Diese Richtlinien können entweder selbst auf den Microsoft-Tenants entsprechend eingerichtet werden, oder vom zentralen CCCS des Ministeriums abgerufen werden.

Die gesetzlichen Grundlagen erlauben den Eltern ein Opt-Out aus den Richtlinien. Diese Möglichkeit des Opt-Out wird über das Bildungsportal angeboten und ist von den Schulen verpflichtend umzusetzen.

- Wurden die Richtlinien manuell eingerichtet, und wurde keine Verbindung zum CCCS initiiert, so erhält die Direktion bzw. der Systemadministrator (laut Bildungsportal) jeweils ein Mail, welcher Schüler bei welcher Richtlinie auszunehmen ist.

- Wurde der Tenant über das Bildungsportal mit dem CCCS verbunden und das lokale Active Directory bzw. Azure Active Directory entsprechend vorbereitet, so geschieht dies automatisch. Dies ist die empfohlene Vorgehensweise.

3 Vorbereitung des Tenants

Damit der Austausch automatisch erfolgt, muss

- im Active Directory (bzw. in weiterer Folge im Azure Active Directory) jeder Schüler entsprechend markiert werden. Dies geschieht bei Schulen mit Server am einfachsten mit dem VOBS-Tool [Prepare AD User](#), bei serverlosen Schulen kann das über die VOBS Tools (<https://tools.vobs.at>) gemacht werden.
- der Tenant mit dem CCCS verbunden werden: <https://bildungsministerium.atlassian.net/wiki/external/Y2E4YmU1ODI4MGU1NDM4OWFmOWFkNWl1NTJINmY3YTl>

4 Umstellung auf die CCCS-Profile

Die bisher von unserer Seite empfohlene Einstellung hat den Kinderschutz bereits beinhaltet. Die CCCS-Profile haben den Vorteil, dass Änderungen dieser Richtlinien umgehend an alle angeschlossenen Tenants verteilt werden. Wenn der Tenant mit dem CCCS verbunden wurde, so erscheinen nach einiger Zeit (1-48 Stunden) neue Richtlinien und neue Gruppen im Intune Admin Center:

Im Wesentlichen decken die CCCS-Profile drei Bereiche ab:

- **Windows Store deaktivieren**
- **Anlegen einer Lokalen Administrators**
- **Web-Inhaltsfilterung**

Richtlinien: Geräte → Windows → Konfiguration

CCCS-Win-ErstellungDeviceTags	Windows 10 und höher	Benutzerdefiniert	23.4.2026, 16:15:55
CCCS-Win-ErstellungDeviceTagsExclusion	Windows 10 und höher	Benutzerdefiniert	4.9.2026, 22:07:47
CCCS-Win-Laps	Windows 10 und höher	Local admin password solution (Win	23.4.2026, 16:15:56
CCCS-Win-LocalAdmins	Windows 10 und höher	Local user group membership	23.4.2026, 16:15:56
CCCS-Win-MSStoreDeaktivieren	Windows 10 und höher	Einstellungenkatalog	23.4.2026, 16:15:54
CCCS-Win-Netzwerkschutz&SmartScreen	Windows 10 und höher	Einstellungenkatalog	23.4.2026, 16:15:58
CCCS-Win-Webfilter-Chrome	Windows 10 und höher	Einstellungenkatalog	4.9.2026, 22:07:49
CCCS-Win-Webfilter-Firefox	Windows 10 und höher	Benutzerdefiniert	4.9.2026, 22:07:50

Diesen neuen CCCS-Richtlinien wurden jeweils automatisch eine entsprechende eingeschlossene Gruppe (Inclusion) und eine entsprechende ausgeschlossene Gruppe (Exclusion) zugewiesen.

Beispiel: Richtlinie CCCS-Win-MSStoreDeaktivieren

[Zuweisungen](#) [Bearbeiten](#)

Eingeschlossene Gruppen

Gruppe	Status	Filter	Filtermodus
CCCS-Win-BlockMSStoreDevices-Inclusion	Aktiv	Keine	Keine

Ausgeschlossene Gruppen

Gruppe	Status
CCCS-Win-BlockMSStoreDevices-Exclusion	Aktiv

Gruppen: Guppen → Alle Gruppen → Filterung CCCS-Win

☐		CCCS-Win-BlockMSStoreDevices-Inclusion	3796322e-0784-448c-87e3-cc74e6fb4769	Sicherheit	Zugewiesen
☐		CCCS-Win-SetEZBAdminDevices-Inclusion	51185630-eb9f-4c7b-a261-10fa592ca37d	Sicherheit	Zugewiesen
☐		CCCS-Win-BlockMSStoreDevices-Exclusion	5c0a3576-3e61-493e-8376-b2edb5249ac7	Sicherheit	Zugewiesen
☐		CCCS-Win-SetEZBAdminDevices-Exclusion	62350106-9f5b-4f73-a20c-676033552167	Sicherheit	Zugewiesen
☐		CCCS-Win-WebfilterDevices-Inclusion	9e6a9952-e04a-4906-ac64-1d2dfec77743	Sicherheit	Zugewiesen
☐		CCCS-Win-WebfilterDevices-Exclusion	ac31058d-b132-4520-af2c-cb46d26f1f2c	Sicherheit	Zugewiesen

Bei allen CCCS-Win-Gruppen handelt es sich um Computergruppen. Diese sind standardmäßig NICHT befüllt, weswegen die Richtlinien auch KEINE Auswirkungen haben. Erst wenn die CCCS-Gruppe Inclusion befüllt wird (z.B. C_T25SuS, C_T26SuS), wird auch die entsprechende Richtlinie wirksam.

4.1 Windows Store blockieren

Vor der Umstellung auf diese neuen Richtlinie muss eine allenfalls zuvor selbst erstellte Richtlinie deaktiviert werden, indem die Zuordnung Alle Geräte entfernt wird.

Bei CCCS-Win-MSSStoreDevices-Inclusion werden mit den einzelnen Jahrgangsgeräte Gruppen befüllt. Die Exclusion Gruppe ist in der Richtlinie bereits inbegriffen und wird automatisch über das Bildungsportal aktualisiert. Entscheidet sich ein Elternteil den Store im Bildungsportal für sein Kind zu aktivieren, so gelangt dieser Benutzer direkt in die CCCS-Win-MSSStoreDevices-Exclusion Gruppe und kann den Store wieder verwenden.

The screenshot shows the Microsoft Entra Groups management console. The left sidebar contains navigation options: Übersicht, Alle Gruppen (selected), Insights (Preview), Gelöschte Gruppen, Diagnose und Problembehandlung, Einstellungen (Allgemein, Ablaufdatum, Benennungsrichtlinie), and Aktivität. The main area displays search results for the query 'cccs-win-block'. The search mode is set to 'Enthält' (Contains), and 2 groups were found. The results are as follows:

Name	Objekt-ID	Gruppentyp	Mitgliedertyp
CCCS-Win-BlockMSSStoreDevices-Inclusion	4062f080-73ac-4c18-838d-e8a2c0b27f44	Sicherheit	Zugewiesen
CCCS-Win-BlockMSSStoreDevices-Exclusion	833c54c9-00a0-4bdd-ae28-f8678f92225a	Sicherheit	Zugewiesen

4.2 Web Inhaltsfilterung

Bildungsportal Variante:

Da diese Variante browserbezogen (Chrome, Edge, Firefox) ist und mit einem anderen Browser umgangen werden könnte, setzen wir auf die bisher bewährte Cleanbrowsing-Variante des VOBS (Inhaltsfilterung über die Netzwerkkarte - DNS).

Anleitung Bildungsportal Variante : Webfilter Konfiguration Windows Devices - Confluence

1. Erstellung eines Wartungsskripts laut Anleitung: Cleanbrowsing

Home > Geräte

Geräte | Skripts und Wartungen

Suche

Bedingter Zugriff

Skripts und Wartungen

Analyse von Gruppenrichtlinien

Bereitstellungen

eSIM-Mobilfunkprofile (Vorschau)

Richtliniensätze

Gerätekategorien

Partnerportale

Regeln für die

Hinzu­fügen oder Entfernen von Favoriten durch Drücken von Ctrl+Shift+F

Wartungen Plattformskripts

Erstellen Sie Skriptpakete auf Geräten und führen Sie sie aus, um die wichtigsten Supportprobleme in Ihrer Organisation proaktiv zu finden und zu beheben. Verwenden Sie diese Tabelle, um den Status Ihrer bereitgestellten Skriptpakete anzuzeigen und die Erkennungs- und Wiederherstellungsergebnisse zu überwachen. Die Ergebnisse werden als Anzahl der betroffenen Geräte angezeigt. [Erfahren Sie mehr.](#)

+ Erstellen Aktualisieren Exportieren Spalten

17 Skriptpakete

Suchen Filter hinzufügen

Skriptpaketname	Autor	Status	Ohne P...	Mit Pro...	Proble...	Wieder...	Insgesa...
Cleanbrowsing	SurfaceGo Besitzer	Aktiv	243	4	3	1	29

2. Anschließend wird die Ausschluss-Gruppe CCCS-Win-WebfilterDevices-Exclusion hinzugefügt. Dadurch ist es den Eltern möglich, das Cleanbrowsing auf dem Gerät im Bildungsportal zu deaktivieren.

Home > Geräte | Skripts und Wartungen

Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen.

Bearbeiten: Cleanbrowsing

Azure AD-Gruppen

Zuweisen zu

Ausgewählte Gruppen

C_Autopilot Stündlich

+ Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen

Ausgeschlossene Gruppen

Schließen Sie entweder Geräte oder Gruppen zu den Zuweisungen zum Einschließen oder Ausschließen hinzu.

Ausgewählte Gruppen

+ Wählen Sie die Gruppen aus, die ausgeschlossen werden sollen

Überprüfen und speichern Auswählen

Ändern Sie Ihre Filter, wenn die gesuchten Elemente nicht angezeigt werden.

Suchen

cccs-webfilterDevices

2 Ergebnisse gefunden

Gruppen

Name	E-Mail
☐ CCCS-Win-WebfilterDevices-Inclusio	
☒ CCCS-Win-WebfilterDevices-Exclusio	

Ausgewählt (1)

Zurücksetzen

CCCS-Win-WebfilterDevices-Exclusion

Home > Geräte | Skripts und Wartungen > Cleanbrowsing

Cleanbrowsing | Eigenschaften

Proaktive Korrekturen

Suche

Übersicht

Verwalten

Eigenschaften

Überwachen

Bereichstags Bearbeiten

Standard

Zuweisungen Bearbeiten

Eingeschlossene Gruppen

Ausgewählte Grupp...	Zeitplan	Intervall	Datum und Uhrzeit	Filter
C_Autopilot	Stündlich	Wird jede Stunde wied...		Kein...

Ausgeschlossene Gruppen

Ausgewählte Gruppen

CCCS-Win-WebfilterDevices-Exclusion

Hinzu­fügen oder Entfernen von Favoriten durch Drücken von Ctrl+Shift+F

4.3. Lokale Administratoren konfigurieren

Bildungsportal Variante (LAPS) - Anleitung: Lokale Administratoren Konfigurieren - Confluence

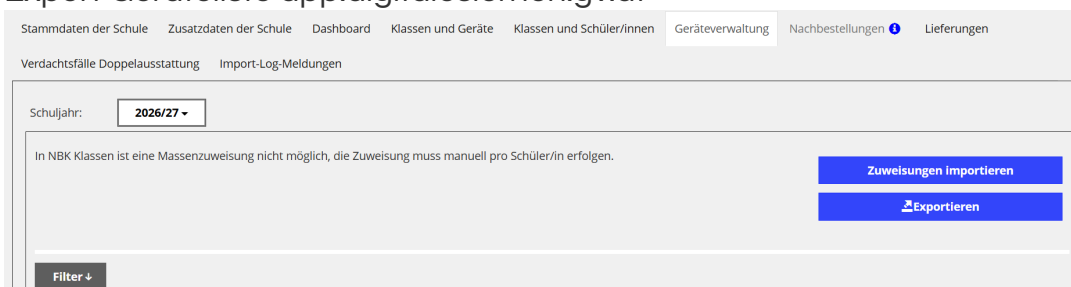
- i** Auch hier setzen wir auf eine eigene VOBS-Variante: Auf jedem Gerät wird ein lokaler Administrator "localhero" mit individuellem Passwort erstellt. Die Eltern erhalten die Daten des lokalen Administrators. Mit dieser Variante ist ein Anmelden mit einem Tenantadmin weiterhin am Gerät möglich. Bei der Bildungsportal Variante ist ein zusätzliches Anmelden nur noch mit dem LAPS-User möglich.

VOBS - Variante für einen lokalen Admin mit tools.vobs.at

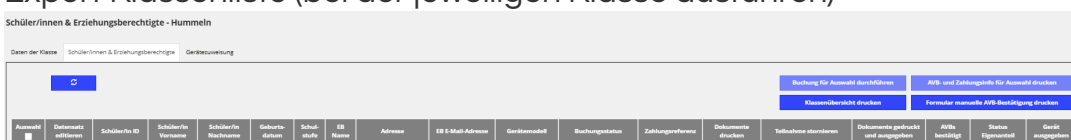
Die Zuordnung Gerät-Hash-Schüler und der Massenimport auf die Seite app.digitaleslernen.gv.at erfolgt seit dem Schuljahr 2026/27 über tools.vobs.at.

4.3.1 Voraussetzungen

- Export Geräteliste app.digitaleslernen.gv.at



- Export Klassenliste (bei der jeweiligen Klasse ausführen)



- tools.vobs.at - oead



Aktiv

OEAD Geräteinitiative

Gerätezuweisung · App-Prüfung · Intune-Hash-Abgleich

Die jeweiligen Listen in den richtigen Feldern hochladen. Die Klassenlisten können einzeln hochgeladen werden (Option B - weitere Klasse anlegen und Excel-Export Datei hochladen) oder die 2-4 Klassenlisten im Vorfeld als ZIP - Verpackungen und bei Option A hochladen.

- Die Hardware-Hash-Liste wird vom VOBS dem jeweiligen MDM Verantwortlichen/Direktion zur Verfügung gestellt. Das ist die dritte Liste zum Hochladen.

Windows: Geräte, Hashes & Klassen
⌵

Präfix / Jahrgang (optional)

Sucht nach 24vorname.nachname@...

GroupTag (optional)

Schuljahr (optional)

HARDWARE-QUELLEDATEIEN

Geräteliste (Excel aus OeAD-Portal)

Datei auswählen

Datei: export_deviceManagement_TW...ZToxMjk3_2026_10_06_3031.xlsx
Entfernen

Hardware Hashes (Excel/CSV)

Datei auswählen

Datei: hash_26.xlsx
Entfernen

SCHÜLER- & KLASSENLISTEN

Option A: Alle Klassen in einer ZIP-Datei

Datei auswählen

ODER

Option B: Klassen einzeln hochladen

Datei auswählen

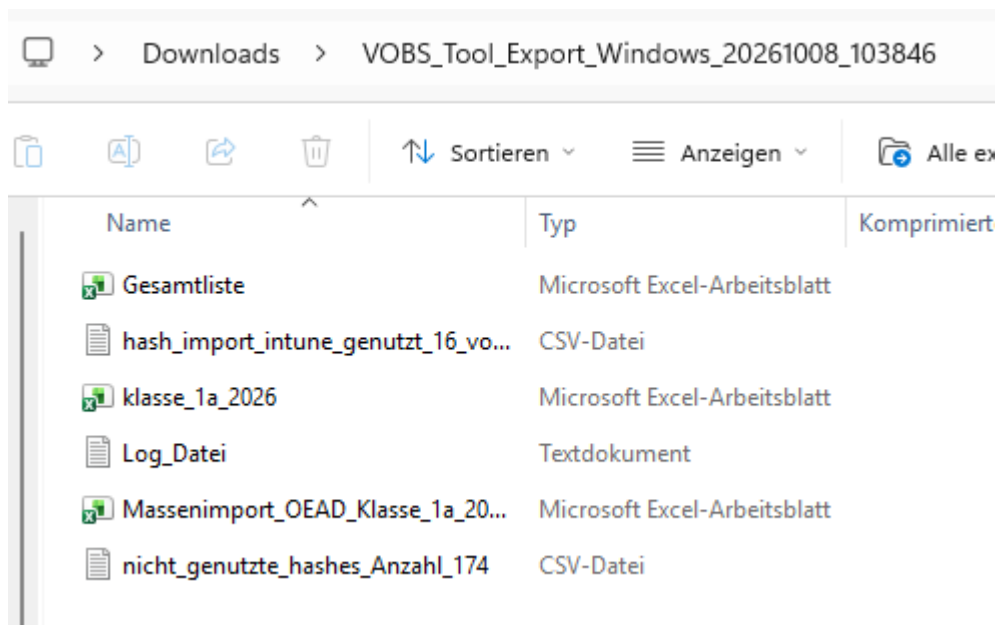
✖

⊕
Weitere Klasse hinzufügen

Windows Verarbeitung starten

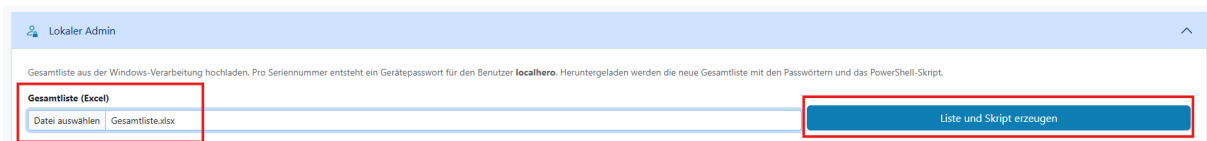
4.3.2 Ergebnis der Verarbeitung

Nach der Verarbeitung erhält man eine Zip - Datei mit folgendem Inhalt:

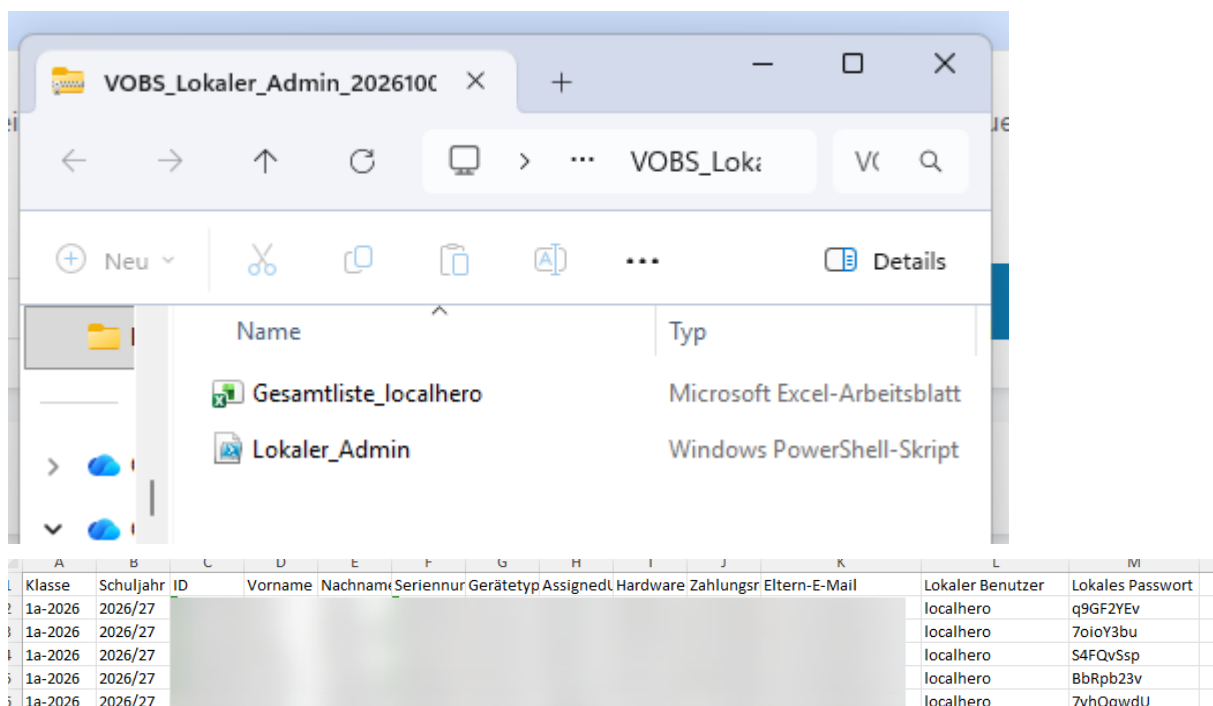


4.3.3 Lokalen Admin erstellen

Hochladen der Gesamtliste aus der ZIP-Datei und Button anklicken



Nun erhält man eine weitere ZIP-Datei mit einer neuen geänderten Gesamtliste: Gesamtliste_localhero.xlsx



Im Script werden keine Passwörter im Klartext gespeichert, sondern auf dem Endgerät automatisiert mit einem entsprechenden Algorithmus erstellt.

4.3.4 Passwortversand an die Eltern

Voraussetzung: Gesamtliste_localhero.xlsx

Gesamtliste öffnen und Liste laden:

Eltern-Mail

Gesamtliste mit der Spalte Lokales Passwort laden, zum Beispiel aus dem Bereich Lokaler Admin. Einzelne Eltern oder eine Auswahl können angeschrieben werden.

Gesamtliste (Excel)

Datei auswählen Gesamtliste_localhero.xlsx

Liste laden

16 Empfänger, 0 ohne Versand.

Alle Keine 16 von 16 ausgewählt

Senden

Senden

Senden

Senden

Senden

Senden

Senden

Absender-Adresse
adresse_des_verantwortlichen_bei_fragen@schule.at

Absender-Name
Vorname und Nachname

Der Mailtext kann angepasst werden.

Zuerst Vorschau vor dem Senden.

Zurück Weiter 1 von 16

Von: Vorname und Nachname

An:

Betreff: Gerätezugang (1a-2026)

Guten Tag,

für das Gerät von (Klasse 1a-2026, Seriennummer) ist ein lokales Administratorkonto eingerichtet.

Benutzername: localhero
Passwort: q9GFZYEv

Bitte behandeln Sie diese Zugangsdaten vertraulich.

Mit freundlichen Grüßen

Anschließend Auswahl senden.

4.3.4 Lokaler_Admin- Skript in Intune einbinden

Das Skript Lokaler_Admin aus der ZIP-Datei wird nun in Intune als Plattformskript bereitgestellt und der betreffenden Gerätegruppe (Bsp: T_26SuS) zugewiesen:



Geräte verwalten

Konfiguration

Kompatibilität

Bedingter Zugriff

Skripts und Wartungen

Analyse von Gruppenrichtlinien

Wartungen

Plattformskripts

+ Hinzufügen

↻ Aktualisieren

↓ Exportieren

≡ Spalten

Filter hinzufügen

Skriptname	Plattform
Lokaler_Admin	Windows



Hier wird keine Exclusion Gruppe hinzugefügt, da wir den lokalen Administrator am Ende der 4. Klasse für das Offboarding benötigen.

5 Quellenangaben

Technischer Kinderschutz - OeAD:

<https://digitaleslernen.oead.at/de/fuer-schulen/geraetemanagement-mdm/technisches-konzept-kinderschutz>

Technischer Kinderschutz - Hauptseite:

<https://bildungsministerium.atlassian.net/wiki/external/M2QyMmNiZTEzYTQ0NDZmYjgwYjY4ODU5YzU2MDcwYmU>

Herstellen der Verbindung zum CCCS:

<https://bildungsministerium.atlassian.net/wiki/external/Y2E4YmU1ODI4MGU1NDM4OWFmOWFkNWl1NTJINmY3YTI>

Aktivieren der automatischen Kinderschutzkonfiguration für Windows:

<https://bildungsministerium.atlassian.net/wiki/external/NGIzYTl0OTFiMDIxNDhjNDhjMWI2ZDQwNmNkMWlwMjk>

Automatische Gruppenzuordnung aktivieren:

<https://bildungsministerium.atlassian.net/wiki/external/MDczYTM2NDY5NDNjNGNIYzliYTlzMzNiZDNjMDM3Mjg>

★Erstellt: 2026-06-02 12:39:20 UTC von Martin Schnetzer
✎Zuletzt aktualisiert: 2026-10-20 08:54:00 UTC von adminalex