

Apple School Manager Connector Dokumentation

Release 6.0.0

Univention GmbH

23.10.2026

Die Quellen dieses Dokuments sind unter der [GNU Affero General Public License v3.0 only](#) lizenziert.

1	Einführung	1
1.1	Zielgruppe dieser Dokumentation	1
1.2	Voraussetzungen	1
1.3	Was der Connector synchronisiert	2
1.4	Passwörter und Geräte	2
2	Installation	3
2.1	Unterstützte Systemrollen	3
2.2	App installieren	3
2.3	SFTP-Zugangsdaten ermitteln	4
2.4	Zugangsdaten eingeben	4
3	Konfiguration	5
3.1	Einstellungsdatei	5
3.2	App-Einstellungen	9
3.3	Synchronisation zeitlich planen	10
3.4	Einstellungen im Detail	10
4	Synchronisation	13
4.1	Synchronisation ausführen	13
4.2	Die CSV-Dateien	14
4.3	Hochgeladene Daten prüfen	16
5	Keycloak als Identity Provider für ASM	17
5.1	Warum Apple School Manager SSF benötigt	17
5.2	Voraussetzungen	17
5.3	Keycloak konfigurieren	18
5.4	Apple School Manager konfigurieren	20
5.5	Auf einem Gerät anmelden	21
6	Fehlerbehebung	23
6.1	Logdatei	23
6.2	Aussagekräftigere Fehlermeldungen von Apple School Manager erhalten	23
6.3	Benutzer erscheinen nicht in Apple School Manager	24
6.4	Apple School Manager lehnt einen Upload ohne Schüler ab	24
6.5	Der Lauf bricht mit einem Fehler bei den Zugangsdaten ab	24
6.6	Der Upload bricht mit einem fehlenden Host-Schlüssel ab	24
6.7	Der Upload in ein Konto bricht mit einem ungültigen LDAP-Filter ab	25
6.8	Klassen haben weniger Lehrer als erwartet	25
6.9	Die Föderation für eine Domain schlägt beim zweiten Mal fehl	25
6.10	Hilfe erhalten	25

7	Changelog	27
7.1	v6.0.0 (2026-10-19)	27
7.2	v5.1.1 (2026-03-05)	27
7.3	v5.1.0	27
7.4	v5.0.3	28
7.5	v5.0.2	28
7.6	v5.0.1	28
7.7	v4.0.0	28
7.8	v3.0.3	28
7.9	v3.0.2	28
7.10	v3.0.1	28
7.11	v2.2.4	28
7.12	v2.2.3	28
7.13	v2.2.2	28
7.14	v2.2.1	28
7.15	v2.2.0	29
7.16	v2.1.0	29
7.17	v2.0.0	29
7.18	v1.2.0	29
7.19	v1.1.0	29
7.20	v1.0.0	29
8	Glossar	31
9	Literaturverzeichnis	33
	Literaturverzeichnis	35
	Stichwortverzeichnis	37

Der *Apple School Manager Connector* ist eine App für *UCS@school*. Er provisioniert die Schulen, Schulklassen, Arbeitsgruppen, Lehrer und Schüler Ihrer UCS@school-Domäne in *Apple School Manager*, sodass Sie dieselben Konten nicht doppelt pflegen müssen.

In diesem Aufbau übernimmt UCS@school die Rolle der Schulverwaltungssoftware, die Apple School Manager erwartet, und der Connector nutzt die SFTP-Schnittstelle, die Apple für solche Systeme bereitstellt. Der Connector sammelt die Daten aus dem LDAP-Verzeichnis, schreibt sie in mehrere CSV-Dateien, packt diese in ein ZIP-Archiv und lädt das Archiv in Apple School Manager hoch.

1.1 Zielgruppe dieser Dokumentation

Diese Dokumentation richtet sich an Administratoren, die eine UCS@school-Domäne betreiben und deren Benutzer in Apple School Manager provisionieren möchten. Sie setzt voraus, dass Sie mit der Administration von *UCS* und UCS@school vertraut sind, insbesondere mit den folgenden Themen:

- Dem *App Center*, siehe *Univention App Center* im UCS-Handbuch [1].
- Der *UCR*, siehe *Administration of local system configuration with Univention Configuration Registry* im UCS-Handbuch [1].
- Den Schulobjekten, die UCS@school verwaltet, siehe *UCS@school-Objekte im LDAP-Verzeichnisdienst* im UCS@school-Handbuch [2].

1.2 Voraussetzungen

Stellen Sie vor Beginn sicher, dass Folgendes vorhanden ist:

- Eine UCS@school-Domäne mit mindestens einer Schule.
- Ein Konto bei Apple School Manager für eine Bildungseinrichtung.
- Die SFTP-Zugangsdaten für das Konto bei Apple School Manager. *SFTP-Zugangsdaten ermitteln* beschreibt, wo Sie diese finden.
- Eine primäre E-Mail-Adresse für jeden Benutzer. Apple School Manager verwendet die E-Mail-Adresse als Apple Account und kann für Benutzer ohne E-Mail-Adresse kein Konto anlegen.

1.3 Was der Connector synchronisiert

Der Connector überträgt Daten nur in eine Richtung, von UCS@school zu Apple School Manager. Er liest niemals Daten zurück und ändert niemals Objekte in Ihrer UCS@school-Domäne.

Die folgende Tabelle zeigt, welche Objekte der Connector auf welche Entität in Apple School Manager abbildet.

Tab. 1.1: Objekte, die der Connector synchronisiert

UCS@school-Objekt	Entität in Apple School Manager
Schule	Standort
Schulklasse oder Arbeitsgruppe	Kurs und Klasse
Schüler	Schüler
Lehrer und Lehrer mit Mitarbeiterrolle	Mitarbeiter
Mitgliedschaft eines Schülers in einer Schulklasse oder Arbeitsgruppe	Roster-Eintrag

Apple School Manager verlangt, dass jede Klasse zu einem Kurs gehört. Daher macht der Connector aus jeder Schulklasse und jeder Arbeitsgruppe einen Kurs mit genau einer Klasse darin. Siehe [Kurse](#).

Mitarbeiter ohne Lehrerrolle werden nicht synchronisiert. Prüfungsbenutzer werden ebenfalls nicht synchronisiert.

[Synchronisation](#) beschreibt die Abbildung im Detail, einschließlich der einzelnen CSV-Spalten.

1.4 Passwörter und Geräte

Der Connector überträgt niemals Passwörter. Apple School Manager erzeugt die Passwörter für neue Konten selbst, und Sie verteilen sie von dort aus. [Passwortrichtlinie für Schüler](#) beschreibt, wie Sie die Länge dieser Passwörter beeinflussen.

Für die Geräteverwaltung empfiehlt Univention eine Lösung für Mobile Device Management, die eine Schnittstelle zu Apple School Manager bietet. Der [Univention-Integrationskatalog](#) listet die Lösungen auf, die sich in UCS@school integrieren.

Sie installieren den *Apple School Manager Connector* wie jede andere App aus dem *App Center*. Dieses Kapitel beschreibt, wo Sie ihn installieren können, wie Sie ihn installieren und wie Sie die Zugangsdaten erhalten, die der Connector benötigt.

2.1 Unterstützte Systemrollen

Sie können den Connector auf den folgenden Systemrollen installieren:

- Primary Directory Node
- Backup Directory Node
- Replica Directory Node

Vorsicht

Installieren Sie den Connector auf genau einem System in der Domäne.

Jede Installation lädt einen vollständigen Datensatz hoch und überschreibt, was der vorherige Upload übertragen hat. Zwei Installationen überschreiben daher gegenseitig ihre Daten. Wenn Sie weitere Schulen synchronisieren möchten, fügen Sie diese der bestehenden Installation hinzu, wie in *Schulen* beschrieben, oder fügen Sie ein weiteres Konto in Apple School Manager hinzu, wie in *Konten in Apple School Manager* beschrieben.

Auf dem Replica Directory Node einer Schule sieht der Connector nur die Schule dieses Nodes. Auf einem zentralen Replica Directory Node, einem Primary Directory Node oder einem Backup Directory Node sieht er alle Schulen der Domäne.

2.2 App installieren

1. Öffnen Sie das App Center in *UMC*.
2. Wählen Sie *Apple School Manager Connector*.
3. Klicken Sie auf *Installieren*.

Beschaffen Sie nach der Installation die Zugangsdaten, wie im nächsten Abschnitt beschrieben, und tragen Sie sie ein, wie in *Zugangsdaten eingeben* beschrieben.

Bemerkung

Der Connector erfordert UCS@school in Version 5.2v5 oder höher. Auf einem System mit einer älteren Version verweigert die App das Update.

2.3 SFTP-Zugangsdaten ermitteln

Apple School Manager erzeugt den SFTP-Benutzernamen und das Passwort für Sie. Um diese zu finden, gehen Sie wie folgt vor:

1. Melden Sie sich bei [Apple School Manager](#) an.
2. Klicken Sie unten links auf Ihren Namen und wählen Sie *Preferences*.
3. Wählen Sie *Managed Apple Accounts*.
4. Öffnen Sie das Menü für *Apple formatted CSV*.
5. Klicken Sie auf *Upload CSV*.

Ein neuer Bereich öffnet sich und zeigt die Daten des SFTP-Kontos. Hintergrundinformationen finden Sie in Apple Inc. [3].

2.4 Zugangsdaten eingeben

1. Speichern Sie das Passwort in `/etc/asm.secret`, mit Leserechten nur für den Benutzer `root`.

Quellcode 2.1: Passwort speichern

```
$ install -m 600 /dev/null /etc/asm.secret
$ editor /etc/asm.secret
```

2. Tragen Sie den Benutzernamen, den Pfad der Passwortdatei und die Schulen in die Einstellungsdatei `/etc/asm-connections.json` ein, die die Installation ohne Konto anlegt.

Quellcode 2.2: Ein Konto in Apple School Manager in `/etc/asm-connections.json`

```
{
  "accounts": {
    "main": {
      "username": "sftp-user",
      "password_file": "/etc/asm.secret"
    }
  },
  "schools": {
    "*": {"account": "main"}
  }
}
```

Der Eintrag `*` in `schools` synchronisiert jede Schule in das Konto.

Einstellungsdatei beschreibt die Datei im Detail, einschließlich der Beschränkung des Kontos auf einzelne Schulen, des Hinzufügens weiterer Konten und aller Einstellungen für Benutzer und Klassen. Fahren Sie danach mit *Konfiguration* fort.

Konfiguration

Der Connector liest seine Konfiguration aus zwei Quellen. Die Einstellungsdatei `/etc/asm-connections.json` enthält die Konten in Apple School Manager, die Schulen, die der Connector in jedes dieser Konten synchronisiert, und alle Einstellungen, die steuern, welche Benutzer der Connector exportiert und wie er ihre Attribute abbildet. Die App-Einstellungen im *App Center* enthalten den Zeitplan der Synchronisation und einige Schalter für den täglichen Betrieb.

Vorsicht

Apple School Manager verwendet die E-Mail-Adresse eines Benutzers als Apple Account. Stellen Sie sicher, dass jeder synchronisierte Benutzer eine primäre E-Mail-Adresse hat. Für Benutzer ohne primäre E-Mail-Adresse kann Apple School Manager kein Konto anlegen. Siehe *E-Mail-Adressen*.

3.1 Einstellungsdatei

Die Einstellungsdatei `/etc/asm-connections.json` hat drei Abschnitte:

accounts

Die Konten in Apple School Manager, jedes mit seinen Zugangsdaten und den Einstellungen für die Schüler und Lehrer, die das Konto erhält. Siehe *Konten in Apple School Manager*.

schools

Die zu synchronisierenden Schulen, jede mit dem Konto, das sie erhält, und den Einstellungen für ihre Klassen. Siehe *Schulen*.

defaults

Einstellungen, die für jedes Konto und jede Schule gelten, sofern ein Konto- oder Schuleintrag sie nicht selbst setzt. Siehe *Voreinstellungen*.

Quellcode 3.1: Zwei Konten in Apple School Manager in `/etc/asm-connections.json`

```
{
  "accounts": {
    "north": {
      "username": "sftp-user-north",
      "password_file": "/etc/asm-north.secret"
```

(Fortsetzung auf der nächsten Seite)

```

    },
    "south": {
        "username": "sftp-user-south",
        "password_file": "/etc/asm-south.secret",
        "student": {"anonymize": false}
    }
},
"defaults": {
    "student": {"password_policy": 6}
},
"schools": {
    "gym123": {"account": "north"},
    "gs456": {
        "account": "south",
        "course_name_pattern": "{name}",
        "student": {"ldap_filter": "(uid=a*)"}
    }
}
}

```

Ein Schüler oder Lehrer, der zu mehreren Schulen desselben Kontos gehört, erscheint im Upload in dieses Konto nur einmal. Die Einstellungen für Schüler und Lehrer gelten daher pro Konto, die Einstellungen für Klassen und die LDAP-Filter pro Schule.

Für jede Einstellung verwendet der Connector den Wert aus dem Konto- oder Schuleintrag, danach den Wert aus `defaults` und danach die eingebaute Voreinstellung.

Die Installation legt die Datei mit Leserechten nur für den Benutzer `root` an. Bearbeiten Sie sie mit einem Texteditor. Der Connector liest die Datei zu Beginn jedes Laufs, daher wirkt eine Änderung ab der nächsten Synchronisation. Er prüft die vollständige Datei, bevor er etwas hochlädt. Die folgenden Probleme brechen den Lauf mit einer Fehlermeldung ab, die die Datei und den Eintrag nennt:

- Eine fehlende Datei oder eine Datei ohne Konto oder ohne Schule.
- Ein fehlender oder unbekannter Schlüssel oder ein Wert vom falschen Typ.
- Eine Schule, die auf ein Konto verweist, das die Datei nicht definiert.
- Eine fehlende oder leere Passwortdatei.
- Ein Benutzername, der bei mehr als einem Konto vorkommt.
- Eine Schule, die nicht existiert, wenn die Datei den Eintrag `*` enthält. Eine falsch geschriebene Schule würde ihre Benutzer sonst an das Konto dieses Eintrags schicken.
- Kein Konto, das eine existierende Schule erhält.

Die folgenden Probleme schreiben nur eine Warnung in die Logdatei. Der Connector lädt in die übrigen Konten hoch:

- Ein Konto, auf das keine Schule verweist. Das Konto erhält keinen Upload.
- Eine Schule, die nicht existiert, wenn die Datei keinen Eintrag `*` enthält. Ein Konto ohne existierende Schule erhält keinen Upload.

Schlägt der Upload in ein Konto fehl, lädt der Connector trotzdem in die übrigen Konten hoch und endet am Schluss mit einem Exit-Status ungleich null.

3.1.1 Konten in Apple School Manager

Der Abschnitt `accounts` ordnet jedem Konto einen Namen Ihrer Wahl zu. Der Name darf nur Buchstaben, Ziffern, `.`, `_` und `-` enthalten. Meist gibt es ein einziges Konto. Wenn die Schulen auf Ihrem UCS@school-System zu verschiedenen Einrichtungen mit jeweils eigenem Konto in Apple School Manager gehören, legen Sie einen Eintrag

pro Konto an. Der Connector lädt dann in jedes Konto ein eigenes Archiv hoch, jeweils beschränkt auf die Schulen, die auf dieses Konto verweisen.

So fügen Sie ein Konto hinzu:

1. Speichern Sie das SFTP-Passwort des Kontos in einer eigenen Datei, die nur `root` lesen kann. [SFTP-Zugangsdaten ermitteln](#) beschreibt, wo Sie das Passwort finden. Jedes Konto hat eigene SFTP-Zugangsdaten und braucht deshalb eine eigene Passwortdatei. Die Beispiele benennen die Datei nach dem Konto, etwa `/etc/asm-north.secret`. Das Konto aus [Zugangsdaten eingeben](#) kann `/etc/asm.secret` behalten.

Quellcode 3.2: Passwort eines Kontos speichern

```
$ install -m 600 /dev/null /etc/asm-north.secret
$ editor /etc/asm-north.secret
```

2. Fügen Sie das Konto dem Abschnitt `accounts` der Einstellungsdatei hinzu.
3. Ordnen Sie dem Konto mindestens eine Schule zu, wie in [Schulen](#) beschrieben.

Ein Kontoeintrag nimmt die folgenden Schlüssel auf. Alle Schlüssel außer `username` und `password_file` sind optional und können auch in `defaults` stehen.

Tab. 3.1: Schlüssel eines Kontoeintrags

Schlüssel	Voreinstellung	Beschreibung
<code>username</code>	Erforderlich	Der SFTP-Benutzername des Kontos.
<code>password_file</code>	Erforderlich	Pfad zur Datei mit dem SFTP-Passwort des Kontos.
<code>email_prepend_domain</code>	Leer	Siehe E-Mail-Adressen .
<code>student.anonymize</code> , <code>staff.anonymize</code>	<code>true</code>	Siehe Anonymisierung .
<code>student.anonymize_values</code> , <code>staff.anonymize_values</code>	Siehe Anonymisierung	Siehe Anonymisierung .
<code>student.person_id_attribute</code> , <code>staff.person_id_attribute</code>	<code>entryUUID</code>	Siehe Identifikation von Benutzern .
<code>student.password_policy</code>	<code>4</code>	Siehe Passwortrichtlinie für Schüler .
<code>student.grade_level_attribute</code>	<code>null</code>	Siehe Jahrgangsstufe von Schülern .

3.1.2 Schulen

Der Abschnitt `schools` führt die zu synchronisierenden Schulen mit ihrem Kürzel auf und ordnet jede von ihnen einem Konto zu. Der Connector synchronisiert nur Schulen, die der Abschnitt aufführt.

Um die Kürzel nachzuschlagen, öffnen Sie *Schul-Administration* ► *Schulen* in der *UMC*. Das Kürzel ist der Name des Schulobjekts, zum Beispiel `gym123`.

Der Eintrag `*` steht für jede Schule, die der Abschnitt nicht namentlich aufführt. Bei einem einzigen Konto synchronisiert er alle Schulen in dieses Konto.

Wenn der Abschnitt eine Schule aufführt, die es nicht gibt, bricht der Connector ab, bevor er etwas hochlädt. Andernfalls ginge eine falsch geschriebene Schule an das Konto des Eintrags `*` statt an das gemeinte Konto.

Quellcode 3.3: Jede Schule in ein Konto, eine Schule mit eigenem LDAP-Filter

```
"schools": {
  "*": {"account": "north"},
  "gym123": {
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

    "account": "north",
    "staff": {"ldap_filter": "(uid=t*)"}
  }
}

```

Ein Schüler oder Lehrer, der zu mehreren Schulen gehört, erscheint im Upload in ein Konto nur mit den Schulen, die zu diesem Konto gehören. Gehört keine seiner Schulen zu dem Konto, überspringt der Connector ihn für dieses Konto.

Ein Schuleintrag nimmt die folgenden Schlüssel auf. Alle Schlüssel außer `account` sind optional und können auch in `defaults` stehen.

Tab. 3.2: Schlüssel eines Schuleintrags

Schlüssel	Voreinstellung	Beschreibung
<code>account</code>	Erforderlich	Name des Kontos im Abschnitt <code>accounts</code> , das die Schule erhält.
<code>course_name_pattern</code>	<code>{ou}-{name}</code>	Siehe <i>Namen von Kursen und Klassen</i> .
<code>class_number_empty</code>	<code>true</code>	Siehe <i>Namen von Kursen und Klassen</i> .
<code>student.ldap_filter</code> , <code>staff.ldap_filter</code>	Leer	Siehe <i>Benutzer mit einem LDAP-Filter auswählen</i> .

3.1.3 Voreinstellungen

Der Abschnitt `defaults` nimmt jeden optionalen Schlüssel eines Konto- und eines Schuleintrags auf. Ein Wert in `defaults` gilt für alle Konten und Schulen, die den Schlüssel nicht selbst setzen.

Quellcode 3.4: Niemanden anonymisieren, außer den Schülern des Kontos

north

```

"defaults": {
  "student": {"anonymize": false},
  "staff": {"anonymize": false}
},
"accounts": {
  "north": {
    "username": "sftp-user-north",
    "password_file": "/etc/asm-north.secret",
    "student": {"anonymize": true}
  }
}

```

3.1.4 Update von einer früheren Version

Bis Version 5.1.1 enthielten App-Einstellungen und UCR-Variablen die Konfiguration. Das Update auf Version 6.0.0 überträgt ihre Werte in die Einstellungsdatei und entfernt die UCR-Variablen. Sie müssen nichts tun. Das Passwort bleibt in `/etc/asm.secret`, und die Einstellungsdatei verweist darauf. Das Konto erhält den Namen `default`.

Tab. 3.3: Bisherige App-Einstellungen und UCR-Variablen

Bisherige Einstellung	Schlüssel in der Einstellungsdatei	
asm/username	accounts.default.username	
asm/password	accounts.default.password_file	
asm/school_whitelist	Ein Eintrag pro Schule in schools oder der Eintrag *, wenn die Liste leer war	
asm/attributes/user/email/ prepend_domain	defaults.email_prepend_domain	
asm/attributes/ROLE/anonymize	defaults.ROLE.anonymize	
asm/attributes/ROLE/anonymize/ATTRIBUTE	defaults.ROLE.anonymize_values. ATTRIBUTE	
asm/attributes/ROLE/person_id/mapping	defaults.ROLE.person_id_attribute, ohne das führende %	
asm/attributes/student/password_policy	defaults.student.password_policy, null für das bisherige –	
asm/attributes/student/grade_level	defaults.student.grade_level_attribute	
asm/attributes/course-name-pattern	defaults.course_name_pattern	
asm/attributes/classes/ class_number_empty	defaults.class_number_empty	
asm/ldap_filter/students, ldap_filter/staff	asm/	defaults.student.ldap_filter, defaults. staff.ldap_filter
asm/ldap_filter/students/SCHOOL, ldap_filter/staff/SCHOOL	asm/	schools.SCHOOL.student.ldap_filter, schools.SCHOOL.staff.ldap_filter

Ersetzen Sie `ROLE` durch `staff` oder `student`, `ATTRIBUTE` durch ein Attribut aus [Anonymisierung](#) und `SCHOOL` durch das Schulkürzel.

Das Update verwirft einen LDAP-Filter für eine Schule, die nicht auf der bisherigen Schulliste stand, weil der Connector diese Schule nicht synchronisiert hat. Außerdem lässt es Schulen weg, die nicht mehr existieren, sowohl aus der bisherigen Schulliste als auch aus den LDAP-Filtern, und gibt für jede einen Hinweis aus.

Ohne `asm/username` hat das Update kein Konto, dem es Schulen zuordnen kann. Es behält `asm/school_whitelist` und die UCR-Variablen `asm/ldap_filter/students/SCHOOL` und `asm/ldap_filter/staff/SCHOOL` und gibt für jede einen Hinweis aus. Übertragen Sie ihre Werte in die Einstellungsdatei, wenn Sie das Konto anlegen.

Wenn `/etc/asm-connections.json` bereits existiert, lässt das Update die Datei und die UCR-Variablen unverändert.

3.2 App-Einstellungen

Um die App-Einstellungen zu öffnen, wählen Sie die App im App Center aus und klicken Sie auf *App-Einstellungen*. Die App-Einstellungen gelten für alle Konten gleichermaßen.

Tab. 3.4: App-Einstellungen des Apple School Manager Connector

Einstellung	Voreinstellung	Beschreibung
asm/sync_daily	False	Führt die Synchronisation einmal am Tag aus. Siehe Synchronisation zeitlich planen .
asm/sync_daily/hour	Nicht gesetzt	Die Stunde des Tages, zu der die tägliche Synchronisation läuft. Gültige Werte sind 0 bis 23.
asm/run_on_appsetting_save	False	Führt die Synchronisation sofort aus, nachdem Sie die App-Einstellungen gespeichert haben.
asm/store_zip	False	Behält das hochgeladene ZIP-Archiv in <code>/var/lib/asm/</code> , statt es nach dem Upload zu löschen.
asm/last_upload	Nicht gesetzt	Schreibgeschütztes Statusfeld. Zeigt an, wann der Connector zuletzt ein Archiv in eines der Konten hochgeladen hat.
asm/last_upload/ACCOUNT	Nicht gesetzt	Zeigt an, wann der Connector zuletzt ein Archiv in das Konto ACCOUNT hochgeladen hat. Nicht Teil der App-Einstellungen.

3.3 Synchronisation zeitlich planen

Der Connector läuft nicht von selbst. Entweder starten Sie ihn manuell, wie in [Synchronisation ausführen](#) beschrieben, oder Sie lassen ihn von einem Cron-Job einmal am Tag ausführen.

Um die tägliche Ausführung zu aktivieren:

1. Öffnen Sie die App-Einstellungen.
2. Wählen Sie `asm/sync_daily` aus.
3. Wählen Sie die Stunde in `asm/sync_daily/hour` aus.
4. Klicken Sie auf *Änderungen anwenden*.

Der Connector schreibt den Cron-Job nach `/etc/cron.d/asm-upload`. Der Job läuft in Minute 0 der gewählten Stunde. Wenn Sie die tägliche Ausführung ohne gültige Stunde aktivieren, schreibt der Connector statt eines Jobs einen Kommentar in die Cron-Datei, und es findet keine Synchronisation statt.

3.4 Einstellungen im Detail

Die folgenden Abschnitte beschreiben die optionalen Schlüssel der Einstellungsdatei. Schlüssel, die mit `student` oder `staff` beginnen, gehören in ein Objekt dieses Namens, wie in `"student": {"anonymize": false}`.

3.4.1 E-Mail-Adressen

Apple School Manager verwendet die E-Mail-Adresse eines Benutzers als Apple Account. Der Connector exportiert die primäre E-Mail-Adresse jedes Benutzers in UCS@school. Benutzer ohne primäre E-Mail-Adresse werden ohne E-Mail-Adresse exportiert, und Apple School Manager kann für sie keinen Apple Account anlegen.

email_prepend_domain

Pro Konto. Fügt den Wert als Subdomain vor der Domain jeder E-Mail-Adresse ein. Mit dem Wert `apple` exportiert der Connector die Adresse `jane@example.com` als `jane@apple.example.com`. Voreinstellung: leer.

3.4.2 Anonymisierung

Wenn Sie die Namen und E-Mail-Adressen Ihrer Benutzer nicht übertragen möchten, können Sie diese anonymisieren. Die Anonymisierung ersetzt die Werte der Attribute `first_name`, `middle_name`, `last_name`, `email_address` und `sis_username` durch Werte, die Sie konfigurieren.

Vorsicht

Ein anonymisierter Benutzer hat keine E-Mail-Adresse, es sei denn, Sie konfigurieren dafür einen Ersatzwert. Ohne E-Mail-Adresse kann Apple School Manager für den Benutzer keinen Apple Account anlegen.

Die Anonymisierung und die Einrichtung aus *Keycloak als Identity Provider für ASM* schließen sich gegenseitig aus. Wenn Sie Keycloak als Identity Provider für Apple School Manager verwenden, deaktivieren Sie die Anonymisierung.

student.anonymize, staff.anonymize

Pro Konto. Aktiviert die Anonymisierung für Schüler und Lehrer. Voreinstellung: `true`.

student.anonymize_values, staff.anonymize_values

Pro Konto. Ersatzwerte für die anonymisierten Attribute. Ein Wert, der mit `%` beginnt, bezeichnet ein LDAP-Attribut, und der Connector exportiert den Wert dieses Attributs aus dem LDAP-Objekt des Benutzers. Ein Wert ohne führendes `%` wird wörtlich exportiert. `null` lässt die Spalte leer. Sie müssen nur die Attribute auflisten, deren Voreinstellung Sie ändern möchten.

Tab. 3.5: Ersatzwerte für anonymisierte Attribute

Schlüssel in <code>anonymize_values</code>	Voreinstellung	Erforderlich
<code>first_name</code>	<code>%uid</code>	Ja
<code>middle_name</code>	<code>null</code>	Nein
<code>last_name</code>	<code>-</code>	Ja
<code>email_address</code>	<code>null</code>	Nein
<code>sis_username</code>	<code>%uid</code>	Nein

Quellcode 3.5: Schüler mit einem festen Nachnamen anonymisieren

```
"student": {
  "anonymize": true,
  "anonymize_values": {"last_name": "Student"}
}
```

3.4.3 Identifikation von Benutzern

Apple School Manager identifiziert einen Benutzer anhand der Spalte `person_id`. Der Connector füllt sie mit einem LDAP-Attribut des Benutzers, das sich nicht ändert, wenn Sie den Benutzer umbenennen.

student.person_id_attribute, staff.person_id_attribute

Pro Konto. LDAP-Attribut, das einen Schüler oder einen Lehrer identifiziert. Voreinstellung: `entryUUID`.

Vorsicht

Ändern Sie diese Schlüssel nicht in einer laufenden Installation. Apple School Manager behandelt einen Benutzer mit einer neuen `person_id` als anderen Benutzer und verliert die Zuordnung zum bestehenden Konto.

3.4.4 Passwortrichtlinie für Schüler

Apple School Manager erstellt das Passwort für einen neuen Schüler selbst. Die Passwortrichtlinie legt fest, wie lang dieses Passwort ist.

student.password_policy

Pro Konto. Länge des Passworts, das Apple für einen neuen Schüler erstellt. Gültige Werte sind 4, 6, 8 und `null`. `null` bedeutet, dass Apple School Manager die Voreinstellung der Schule verwendet. Voreinstellung: 4.

Apple School Manager unterstützt keine Passwortrichtlinie für Lehrer.

3.4.5 Jahrgangsstufe von Schülern

`student.grade_level_attribute`

Pro Konto. LDAP-Attribut, das die Jahrgangsstufe eines Schülers enthält. Der Connector exportiert seinen Wert in der Spalte `grade_level`. Voreinstellung: `null`, wodurch die Spalte leer bleibt.

3.4.6 Namen von Kursen und Klassen

UCS@school stellt dem Namen einer Schulklasse das Schulkürzel voran, zum Beispiel `gym123-1a`. Der Connector leitet den Kursnamen aus diesem Namen ab.

`course_name_pattern`

Pro Schule. Muster für den Kursnamen. Der Connector ersetzt `{ou}` durch das Schulkürzel und `{name}` durch den Klassennamen ohne Schulpräfix. Voreinstellung: `{ou}-{name}`.

`class_number_empty`

Pro Schule. Lässt die Spalte `class_number` leer. Apple School Manager bildet den Namen einer Klasse aus dem Kursnamen und der Klassennummer, daher würde eine gleichlautende Klassennummer den Kursnamen nur wiederholen. Voreinstellung: `true`.

3.4.7 Benutzer mit einem LDAP-Filter auswählen

Wenn die Schulliste aus *Schulen* nicht fein genug ist, können Sie die Benutzer mit einem LDAP-Filter auswählen. Der Connector wendet den Filter zusätzlich zur Schulliste an.

`student.ldap_filter`, `staff.ldap_filter`

Pro Schule. LDAP-Filter für die Schüler oder die Lehrer der Schule. Ein Filter in `defaults` gilt für jede Schule, die keinen eigenen setzt. Voreinstellung: leer, wodurch jeder Benutzer ausgewählt wird.

Quellcode 3.6: Nur die Schüler von `gym123` mit primärer E-Mail-Adresse synchronisieren

```
"gym123": {
  "account": "north",
  "student": {"ldap_filter": "(mailPrimaryAddress=*)"}
}
```

Der Connector kombiniert den Filter mit seiner eigenen Auswahl der Schüler oder Lehrer der Schule, daher muss der Filter nur die Attribute der gewünschten Benutzer beschreiben. Um zu prüfen, welche Benutzer ein Filter auswählt, bevor Sie ihn setzen, kombinieren Sie ihn mit der Rolle der Benutzer und führen Sie ihn mit `univention-ldap-search` aus:

Quellcode 3.7: Die Schüler von `gym123` auflisten, auf die der Filter zutrifft

```
$ univention-ldapsearch -LLL \
'(&(ucsschoolRole=student:school:gym123)(mailPrimaryAddress=*))' uid
```

Vorsicht

Ein ungültiger LDAP-Filter bricht den Upload in das Konto dieser Schule ab. Der Connector lädt in diesem Fall nichts in dieses Konto hoch, daher bleiben dessen Daten in Apple School Manager so, wie sie nach dem letzten erfolgreichen Lauf waren. Die anderen Konten erhalten ihren Upload trotzdem.

Synchronisation

Ein Synchronisationslauf liest die Schuldaten aus dem LDAP-Verzeichnis, schreibt sie in CSV-Dateien, packt die Dateien in ein ZIP-Archiv und lädt das Archiv zu Apple School Manager hoch. Dieses Kapitel beschreibt den Lauf selbst und die Daten, die er überträgt.

4.1 Synchronisation ausführen

Drei Auslöser starten einen Synchronisationslauf:

- Der Cron-Job aus *Synchronisation zeitlich planen*.
- Das Speichern der App-Einstellungen, wenn Sie `asm/run_on_appsetting_save` aktiviert haben.
- Der Befehl **asm-upload** auf der Kommandozeile.

Quellcode 4.1: Synchronisationslauf manuell starten

```
$ /usr/sbin/asm-upload
```

Der Befehl gibt Fortschrittmeldungen im Terminal aus und schreibt ein ausführlicheres Log nach `/var/log/univention/asm.log`. Er endet mit einem Exit-Status ungleich null, wenn die Zugangsdaten fehlen oder der Upload in ein Konto fehlschlägt.

4.1.1 Ablauf eines Synchronisationslaufs

1. Der Connector liest die Einstellungsdatei `/etc/asm-connections.json`, wie in *Einstellungsdatei* beschrieben. Ein fehlender oder ungültiger Eintrag bricht den Lauf ab, ebenso eine Schule, die es im LDAP-Verzeichnis nicht gibt.
2. Der Connector sammelt die Schulen, Schulklassen, Arbeitsgruppen, Lehrer und Schüler aus dem LDAP-Verzeichnis, beschränkt auf die Schulen des Kontos und durch die LDAP-Filter aus *Benutzer mit einem LDAP-Filter auswählen*.
3. Der Connector schreibt die sechs CSV-Dateien aus *Die CSV-Dateien* in ein temporäres Verzeichnis.
4. Der Connector packt die CSV-Dateien in `/var/lib/asm/asm_TIMESTAMP.zip` und entfernt das temporäre Verzeichnis. `TIMESTAMP` ist der Zeitpunkt, zu dem der Connector das Archiv erstellt hat, im Format ISO 8601, zum Beispiel `2026-10-01T03:00:12.345678`.
5. Der Connector öffnet eine SFTP-Verbindung zu `upload.appleschoolcontent.com` und lädt das Archiv als `archive.zip` hoch. Den Host-Schlüssel prüft er gegen `/etc/asm_public_key`.

6. Der Connector setzt `asm/last_upload` und `asm/last_upload/ACCOUNT` auf die aktuelle Uhrzeit und löscht das Archiv, sofern Sie `asm/store_zip` nicht aktiviert haben.

Bei mehreren Konten wiederholt der Connector die Schritte 2 bis 6 für jedes Konto.

Jeder Lauf überträgt den vollständigen Datenbestand. Der Connector verfolgt nicht, was sich seit dem letzten Lauf geändert hat.

4.1.2 Wie Apple School Manager die Daten übernimmt

Apple School Manager vergleicht die hochgeladenen Daten mit den Konten, die es verwaltet:

- Ein Benutzer, der zum ersten Mal auftaucht, erhält ein neues Konto.
- Ein Benutzer, der nicht mehr im Upload enthalten ist, wird sofort deaktiviert und nach 30 Tagen gelöscht.
- Ein Benutzer, dessen Attribute sich geändert haben, behält sein Konto, solange die Spalte `person_id` unverändert bleibt. Siehe [Identifikation von Benutzern](#).

4.2 Die CSV-Dateien

Das Archiv enthält die folgenden sechs Dateien. Apple dokumentiert ihr Format in Apple Inc. [4]. Der Connector sortiert die Zeilen jeder Datei nach Schule und anschließend nach Benutzer- oder Klassenname.

Tab. 4.1: Dateien im hochgeladenen Archiv

Datei	Inhalt
<code>locations.csv</code>	Eine Zeile pro Schule.
<code>courses.csv</code>	Eine Zeile pro Schulklasse und Arbeitsgruppe.
<code>classes.csv</code>	Eine Zeile pro Schulklasse und Arbeitsgruppe, mit den Lehrern dieser Klasse.
<code>staff.csv</code>	Eine Zeile pro Lehrer.
<code>students.csv</code>	Eine Zeile pro Schüler.
<code>rosters.csv</code>	Eine Zeile pro Mitgliedschaft eines Schülers in einer Schulklasse oder Arbeitsgruppe.

4.2.1 Standorte

Tab. 4.2: Spalten von `locations.csv`

Spalte	Quelle in UCS@school
<code>location_id</code>	Name der Schule, zum Beispiel <code>gym123</code> .
<code>location_name</code>	Anzeigenname der Schule. Hat die Schule keinen Anzeigenamen, verwendet der Connector stattdessen den Namen.

4.2.2 Kurse

Apple School Manager verlangt, dass jede Klasse zu einem Kurs gehört. UCS@school kennt nur die Schulklasse oder Arbeitsgruppe, daher exportiert der Connector jede davon zweimal: einmal als Kurs in `courses.csv` und einmal als Klasse dieses Kurses in `classes.csv`. Beide Zeilen verwenden den Namen der Gruppe als ID, sodass jeder Kurs genau eine Klasse hat.

Tab. 4.3: Spalten von `courses.csv`

Spalte	Quelle in UCS@school
<code>course_id</code>	Name der Schulklasse oder Arbeitsgruppe einschließlich des Schulpräfixes, zum Beispiel <code>gym123-1a</code> .
<code>course_number</code>	Derselbe Wert wie <code>course_id</code> .
<code>course_name</code>	Gebildet aus <code>course_name_pattern</code> . Siehe Namen von Kursen und Klassen .
<code>location_id</code>	Name der Schule.

4.2.3 Klassen

Tab. 4.4: Spalten von `classes.csv`

Spalte	Quelle in UCS@school
<code>class_id</code>	Name der Schulklasse oder Arbeitsgruppe.
<code>class_number</code>	Standardmäßig leer. Siehe <code>class_number_empty</code> in <i>Namen von Kursen und Klassen</i> .
<code>course_id</code>	Name der Schulklasse oder Arbeitsgruppe.
<code>instructor_id</code> , <code>instructor_id_2</code> , <code>instructor_id_3</code>	Die <code>person_id</code> der ersten drei Lehrer der Klasse.
<code>instructor_id_4</code> bis <code>instructor_id_15</code>	Die <code>person_id</code> der übrigen Lehrer. Der Connector schreibt nur so viele Spalten, wie er benötigt.
<code>location_id</code>	Name der Schule.

Bemerkung

Apple School Manager unterstützt höchstens 15 Lehrer pro Klasse. Hat eine Klasse mehr, synchronisiert der Connector die ersten 15 und schreibt eine Warnung in die Logdatei.

4.2.4 Mitarbeiter

Tab. 4.5: Spalten von `staff.csv`

Spalte	Quelle in UCS@school
<code>person_id</code>	Das Attribut aus <code>staff.person_id_attribute</code> , standardmäßig <code>entryUUID</code> .
<code>person_number</code>	Derselbe Wert wie <code>person_id</code> .
<code>first_name</code>	Vorname des Lehrers.
<code>middle_name</code>	Erster Wert von <code>middleName</code> , <code>initials</code> oder <code>oxMiddleName</code> .
<code>last_name</code>	Nachname des Lehrers.
<code>email_address</code>	Primäre E-Mail-Adresse, angepasst durch <code>email_prepend_domain</code> .
<code>sis_username</code>	Benutzername des Lehrers.
<code>location_id</code>	Primäre Schule des Lehrers.
<code>location_id_2</code> und folgende	Die weiteren Schulen des Lehrers, in alphabetischer Reihenfolge.

Die Datei enthält Lehrer sowie Lehrer mit zusätzlicher Mitarbeiterrolle. Mitarbeiter ohne Lehrerrolle sind nicht Teil des Exports.

4.2.5 Schüler

Tab. 4.6: Spalten von `students.csv`

Spalte	Quelle in UCS@school
<code>person_id</code>	Das Attribut aus <code>student.person_id_attribute</code> , standardmäßig <code>entryUUID</code> .
<code>person_number</code>	Derselbe Wert wie <code>person_id</code> .
<code>first_name</code>	Vorname des Schülers.
<code>middle_name</code>	Erster Wert von <code>middleName</code> , <code>initials</code> oder <code>oxMiddleName</code> .
<code>last_name</code>	Nachname des Schülers.
<code>grade_level</code>	Das Attribut aus <code>student.grade_level_attribute</code> . Leer, wenn der Schlüssel nicht gesetzt ist.
<code>email_address</code>	Primäre E-Mail-Adresse, angepasst durch <code>email_prepend_domain</code> .
<code>sis_username</code>	Benutzername des Schülers.
<code>password_policy</code>	Der Wert von <code>student.password_policy</code> . Siehe Passwortrichtlinie für Schüler .
<code>location_id</code>	Primäre Schule des Schülers.
<code>location_id_2</code> und folgende	Die weiteren Schulen des Schülers, in alphabetischer Reihenfolge.

Prüfungsbenutzer sind nicht Teil des Exports.

4.2.6 Roster

Tab. 4.7: Spalten von `rosters.csv`

Spalte	Quelle in UCS@school
<code>roster_id</code>	Der Klassenname und die <code>person_id</code> des Schülers, verbunden durch einen Bindestrich.
<code>class_id</code>	Name der Schulklasse oder Arbeitsgruppe.
<code>student_id</code>	Die <code>person_id</code> des Schülers.

Die Datei enthält nur Schüler. Lehrer werden einer Klasse über die Spalten `instructor_id` von `classes.csv` zugeordnet.

4.3 Hochgeladene Daten prüfen

Um zu sehen, was der Connector hochlädt, aktivieren Sie `asm/store_zip` in den App-Einstellungen und führen Sie die Synchronisation aus. Der Connector behält das Archiv dann in `/var/lib/asm/`.

Quellcode 4.2: Archive auflisten und das neueste entpacken

```
$ ls -l /var/lib/asm/
$ unzip -d /var/tmp/asm "$(ls -t /var/lib/asm/*.zip | head -1)"
```

Vorsicht

Die Archive enthalten personenbezogene Daten. Löschen Sie sie, sobald Sie sie nicht mehr benötigen, und deaktivieren Sie `asm/store_zip` wieder.

Keycloak als Identity Provider für ASM

Apple School Manager kann die Anmeldung seiner Managed Apple Accounts an einen externen Identity Provider fördern. Ihre Benutzer melden sich dann an ihren Apple-Geräten mit dem Passwort aus Ihrer UCS@school-Domäne an statt mit einem Passwort, das Apple School Manager verwaltet.

Dieses Kapitel beschreibt, wie Sie die *Keycloak*-App von UCS als diesen Identity Provider einrichten.

Vorsicht

Die *SSF*-Unterstützung, die Apple School Manager voraussetzt, ist ein experimentelles Feature von Keycloak.

5.1 Warum Apple School Manager SSF benötigt

Das Shared Signals Framework ist der Standard der OpenID Foundation für den Austausch von Sicherheitsereignissen, Zustandsänderungen und Risikosignalen zwischen einem Identity Provider und den Anwendungen, die sich auf ihn stützen. Siehe OpenID Foundation [5].

Apple School Manager nutzt SSF, um von Ereignissen in Ihrer Domäne zu erfahren, etwa von geänderten Anmeldedaten oder einer widerrufenen Sitzung. Deshalb akzeptiert es nur einen Identity Provider, der als SSF-Transmitter agiert. Ein einfacher *OIDC*-Client genügt nicht.

5.2 Voraussetzungen

- Eine UCS@school-Domäne mit dem Apple School Manager Connector und der Keycloak-App in Version 26.7.2-nubus1 oder neuer.
- Eine Domain, die Sie in Apple School Manager verifiziert haben. Siehe Apple Inc. [6]. Ihre Benutzer benötigen eine primäre E-Mail-Adresse in dieser Domain, um sich anzumelden.
- Ein Konto in Apple School Manager mit der Rolle *Administrator*, um den Identity Provider zu verbinden. Siehe Apple Inc. [7]. Dieses Konto kann sich selbst nicht über die Föderation anmelden.
- Ein Apple-Gerät für die erste Anmeldung.
- Deaktivierte Anonymisierung, weil Apple School Manager die E-Mail-Adresse als Apple Account benötigt:

Quellcode 5.1: Anonymisierung in `/etc/asm-connections.json` ausschalten

```
"defaults": {
  "student": {"anonymize": false},
  "staff": {"anonymize": false}
}
```

Siehe *Anonymisierung*.

5.3 Keycloak konfigurieren

Nehmen Sie alle Einstellungen in der Keycloak-Administrationskonsole im Realm `ucs` vor, der die Benutzer Ihrer Domäne enthält. Die Administrationskonsole öffnet sich im Realm `master`. Wählen Sie den Realm `ucs` aus, bevor Sie etwas ändern, und prüfen Sie den ausgewählten Realm, wann immer Sie zur Administrationskonsole zurückkehren.

5.3.1 SSF-Feature aktivieren

Setzen Sie die App-Einstellung `keycloak/server/feature/ssf` der Keycloak-App auf `true`.

1. Öffnen Sie das App Center in der *UMC* und wählen Sie die Keycloak-App aus.
2. Klicken Sie auf *App settings*.
3. Wählen Sie `keycloak/server/feature/ssf` aus.
4. Klicken Sie auf *Apply changes*.

Alternativ können Sie die Einstellung auf der Kommandozeile setzen:

Quellcode 5.2: SSF-Feature von Keycloak aktivieren

```
$ univention-app configure keycloak --set keycloak/server/feature/ssf=true
```

Das App Center erstellt daraufhin den Keycloak-Container neu, der Keycloak mit dem SSF-Feature startet. Währenddessen ist Keycloak für kurze Zeit nicht erreichbar.

Bemerkung

Wenn Sie die Variable stattdessen mit `ucr set` setzen, übernehmen Sie sie mit `univention-app configure keycloak`. Ein Neustart der App mit `univention-app restart keycloak` reicht nicht aus, und die Seite *Realm settings* bietet *SSF Transmitter* nicht an.

5.3.2 Realm zum SSF-Transmitter machen

1. Öffnen Sie die Keycloak-Administrationskonsole unter `https://ucs-sso-ng.DOMAIN/admin/` und wählen Sie den Realm `ucs` aus. Ersetzen Sie `DOMAIN` durch den Domänennamen Ihrer UCS-Domäne.
2. Setzen Sie auf der Seite *Realm settings* die Option *SSF Transmitter* auf *On*.

Sobald *SSF Transmitter* aktiviert ist, bietet der Realm neben der OpenID-Endpunktconfiguration einen Endpunkt für die SSF-Konfigurationsmetadaten an. Die URLs beider Endpunkte benötigen Sie in *Identity Provider verbinden*:

- `https://ucs-sso-ng.DOMAIN/realms/ucs/.well-known/openid-configuration`
- `https://ucs-sso-ng.DOMAIN/realms/ucs/.well-known/ssf-configuration`

Die URLs verwenden die Standardwerte der Keycloak-App: den Host `ucs-sso-ng.DOMAIN` und den Realm `ucs`, der die Benutzer der Domäne enthält. Wenn Sie `keycloak/server/sso/fqdn` geändert haben oder einen anderen Realm verwenden, passen Sie die URLs entsprechend an.

5.3.3 Client Scopes anlegen

Legen Sie auf der Seite *Client scopes* des Realms die Client Scopes `ssf.manage` und `ssf.read` an, jeweils mit aktivierter Option *Include in token scope*.

5.3.4 OIDC-Client anlegen

1. Klicken Sie auf der Seite *Clients* des Realms auf *Create client*.
2. Geben Sie auf der Seite *General settings* `apple-asm` als *Client ID* ein.
3. Tragen Sie auf der Seite *Capability config* die Einstellungen aus der folgenden Tabelle ein.

Tab. 5.1: Fähigkeiten des OIDC-Clients für Apple School Manager

Einstellung	Wert
<i>Client authentication</i>	<i>On</i>
<i>Authentication flow</i>	<i>Standard flow</i>
<i>Require PKCE</i>	<i>Off</i>
<i>SSF Receiver</i>	<i>On</i>

Apple scheint *PKCE* für OIDC-Föderationen nicht zu unterstützen, weshalb der Client es deaktiviert. Die Seite bietet *SSF Receiver* erst an, wenn *Client authentication* aktiviert ist und Sie *SSF-Feature aktivieren* und *Realm zum SSF-Transmitter machen* abgeschlossen haben.

4. Tragen Sie auf der Seite *Login settings* die Einstellungen aus der folgenden Tabelle ein und klicken Sie auf *Save*.

Tab. 5.2: Anmeldeeinstellungen des OIDC-Clients für Apple School Manager

Einstellung	Wert
<i>Valid redirect URIs</i>	<code>https://gsa-ws.apple.com/grand slam/GsService2/acs</code>
<i>Valid post logout redirect URIs</i>	<code>+</code>

Kopieren Sie das Client Secret aus dem Reiter *Credentials*. Sie benötigen es in *Identity Provider verbinden*.

5.3.5 Client als SSF-Receiver konfigurieren

1. Fügen Sie im Reiter *Client scopes* des Clients `ssf.manage`, `ssf.read` und `offline_access` als *Default* hinzu.
2. Fügen Sie im Reiter *Roles* die Client-Rolle `ssf-admin` hinzu.
3. Tragen Sie im Reiter *SSF* die Einstellungen aus der folgenden Tabelle ein.

Tab. 5.3: SSF-Einstellungen des Clients

Einstellung	Wert
<i>Profile</i>	<i>SSE CAEP 1.0</i>
<i>Default Subjects</i>	NONE
<i>Subject format</i>	iss_sub
<i>Add subject on login</i>	On
<i>Auto verify stream</i>	On
<i>Verification delay</i>	1500
<i>Required role</i>	Klicken Sie auf <i>Select role</i> , wählen Sie <i>Client roles</i> und wählen Sie <i>ssf-admin</i> aus.
<i>Allowed delivery methods</i>	Nur <i>Push Delivery</i>
<i>Valid push URLs</i>	<code>https://federation.apple.com/feeds/school/caep/*</code>
<i>Supported Events</i>	CaepCredentialChange, CaepSessionRevoked
<i>Emit events enabled</i>	On
<i>Emit-only events</i>	CaepSessionRevoked

Auto verify stream sendet das Verifizierungsereignis, sobald Apple den Stream anlegt. Mit *Emit-only events* steuern Sie über die Keycloak-API, wann Keycloak eine Abmeldung an Apple sendet.

5.3.6 Administrativen Benutzer anlegen

Apple School Manager baut die Verbindung zu Keycloak mit dem Authorization Code Flow auf. Das resultierende Access Token und Refresh Token gehören zu einer Offline-Sitzung eines Benutzers, daher muss dieser Benutzer existieren, bevor Sie die beiden Systeme verbinden.

Legen Sie den Benutzer in Keycloak an, nicht in UCS. Keycloak hat nur Lesezugriff auf die Benutzer aus UCS und kann ihnen deshalb keine Client-Rollen zuweisen.

1. Legen Sie im Realm `ucs` einen Benutzer an, zum Beispiel `asm`.
2. Setzen Sie Vorname, Nachname und E-Mail-Adresse.
3. Setzen Sie im Reiter *Credentials* ein starkes Passwort. Zwei-Faktor-Authentifizierung ist optional, aber empfohlen.
4. Weisen Sie die Client-Rolle `ssf-admin` des Clients `apple-asm` zu.

5.4 Apple School Manager konfigurieren

5.4.1 Identity Provider verbinden

1. Melden Sie sich bei [Apple School Manager](#) an.
2. Öffnen Sie *Preferences* ▶ *Managed Apple Accounts*.
3. Stellen Sie sicher, dass Ihre Domain verifiziert ist.
4. Klicken Sie unter *User sign-in and directory sync* auf *Configure*. Wenn bereits ein anderer Identity Provider verbunden ist, trennen Sie diesen zuerst.
5. Wählen Sie *Custom Identity Provider* aus und klicken Sie auf *Continue*.
6. Geben Sie einen Namen für den Identity Provider ein, zum Beispiel `asmkc`.
7. Geben Sie die Client-ID und das Client Secret aus *OIDC-Client anlegen* sowie die beiden URLs aus *Realm zum SSF-Transmitter machen* ein, wie in der folgenden Tabelle aufgeführt.

Tab. 5.4: Einstellungen des benutzerdefinierten Identity Providers in Apple School Manager

Feld	Wert
<i>Client ID</i>	apple-asm
<i>Client Secret</i>	Das Client Secret aus dem Reiter <i>Credentials</i> des Clients
<i>SSF URL</i>	https://ucs-sso-ng.DOMAIN/realms/ucs/.well-known/ssf-configuration
<i>OIDC URL</i>	https://ucs-sso-ng.DOMAIN/realms/ucs/.well-known/openid-configuration

8. Klicken Sie auf *Continue*.
9. Klicken Sie im sich öffnenden Fenster auf die Anmeldeschaltfläche Ihres Identity Providers, zum Beispiel *Sign in with asmkc*.
10. Melden Sie sich mit dem administrativen Benutzer aus *Administrativen Benutzer anlegen* an.

Apple School Manager zeigt *Authorizing Account* an und bestätigt dann die Verbindung. Beim Verbinden legt Apple einen SSF-Stream für den Client an, den Sie in Keycloak im Reiter *SSF Streams* des Clients sehen.

5.4.2 Föderation für die Domain aktivieren

1. Öffnen Sie *Preferences* ▶ *Managed Apple Accounts*.
2. Wählen Sie Ihre Domain aus und klicken Sie auf *Manage*.
3. Suchen Sie unten auf der Seite den Abschnitt für Ihren Identity Provider und klicken Sie auf *Set up*.
4. Stellen Sie den erscheinenden Schalter auf *On*.
5. Wenn der SFTP-Upload die Domain verwendet, fordert Apple School Manager Sie auf, eine andere Domain für den Upload zu wählen. Wählen Sie eine beliebige andere Domain.

Apple School Manager aktiviert die Föderation für die Domain und sendet eine Bestätigungs-E-Mail.

Danach meldet sich jeder Managed Apple Account mit einer E-Mail-Adresse in der Domain über Keycloak an. Das gilt auch für Konten, die es bereits vor der Aktivierung der Föderation gab, und für Konten, die Sie in Apple School Manager manuell angelegt haben.

Der Upload des Connectors funktioniert weiterhin. Apple School Manager ordnet die Konten anhand der Domain ihrer E-Mail-Adresse zu, sodass die Konten aus dem Upload zur föderierten Domain gehören, unabhängig von der Domain, die Sie für den SFTP-Upload gewählt haben.

5.5 Auf einem Gerät anmelden

Nachdem Sie die Föderation für die Domain aktiviert haben, melden sich Ihre Benutzer mit ihren UCS@school-Anmeldedaten an einem Apple-Gerät an. Die folgenden Schritte beschreiben ein nicht gekoppeltes Gerät. Das allgemeine Vorgehen beschreibt Apple Inc. [8].

1. Öffnen Sie *Settings* ▶ *Apple Account*.
2. Tippen Sie auf *Sign In Manually*.
3. Geben Sie die E-Mail-Adresse des Benutzers in der föderierten Domain ein und tippen Sie auf *Proceed*.
4. Das Gerät zeigt einen Hinweis an, der Ihre Organisation nennt. Tippen Sie auf *Proceed*.
5. Die Keycloak-Anmeldeseite öffnet sich mit bereits ausgefülltem Benutzernamen. Geben Sie das Passwort ein.
6. Geben Sie die Geräte-PIN ein, wenn das Gerät danach fragt.

Nach der Anmeldung zeigt *Settings* ▶ *Apple Account* den Benutzer mit der E-Mail-Adresse aus UCS@school an.

Fehlerbehebung

Dieses Kapitel beschreibt, wo der Connector protokolliert, was er tut, und was Sie bei den häufigsten Problemen tun können.

6.1 Logdatei

Der Connector schreibt in `/var/log/univention/asm.log`. Die Datei enthält das Log jedes Laufs auf Debug-Level, einschließlich der Lehrer, die ein LDAP-Filter aus einer Klasse ausgeschlossen hat. Die App-Einstellungen zeigen den Zeitpunkt des letzten Uploads in `asm/last_upload.asm/last_upload/ACCOUNT` enthält den Zeitpunkt des letzten Uploads in jedes Konto.

Die Logrotation richtet sich nach den UCR-Variablen `logrotate/*` des Systems. Der Connector schreibt seine eigene Konfiguration nach `/etc/logrotate.d/asm`.

Quellcode 6.1: Synchronisationslauf verfolgen

```
$ tail -f /var/log/univention/asm.log
```

6.2 Aussagekräftigere Fehlermeldungen von Apple School Manager erhalten

Apple School Manager meldet Fehler in den hochgeladenen Daten nur spärlich. Die Seite, die die SFTP-Zugangsdaten anzeigt, gibt genauer an, welche Daten Apple School Manager ablehnt. Der SFTP-Upload kann dabei verbunden bleiben.

1. Öffnen Sie die Seite mit den SFTP-Zugangsdaten, wie in *SFTP-Zugangsdaten ermitteln* beschrieben.
2. Lassen Sie die Seite geöffnet und starten Sie einen Synchronisationslauf, wie in *Synchronisation ausführen* beschrieben.

Die Seite zeigt die Fehler jedes Uploads an, während der Upload läuft.

6.3 Benutzer erscheinen nicht in Apple School Manager

Prüfen Sie Folgendes in dieser Reihenfolge:

1. **Der Benutzer hat keine primäre E-Mail-Adresse.** Der Connector exportiert den Benutzer ohne E-Mail-Adresse, und Apple School Manager kann für den Benutzer keinen Apple Account anlegen.
2. **Die Anonymisierung hat die E-Mail-Adresse entfernt.** Die Anonymisierung ist standardmäßig aktiviert. Ist `student.anonymize` oder `staff.anonymize` für das Konto aktiviert, exportiert der Connector statt der Adresse den Ersatzwert, der standardmäßig leer ist. Siehe [Anonymisierung](#).

Quellcode 6.2: Anonymisierung in `/etc/asm-connections.json` ausschalten

```
"defaults": {
  "student": {"anonymize": false},
  "staff": {"anonymize": false}
}
```

3. **Die Schule steht nicht auf der Liste.** Der Connector exportiert nur Schulen, die der Abschnitt `schools` der Einstellungsdatei aufführt, und nur in das Konto, auf das die Schule verweist. Siehe [Schulen](#).
4. **Ein LDAP-Filter schließt den Benutzer aus.** Die Logdatei nennt keine Benutzer, die ein Filter ausgeschlossen hat. Führen Sie den Filter mit `univention-ldapsearch` aus, um zu prüfen, welche Benutzer er auswählt. Siehe [Benutzer mit einem LDAP-Filter auswählen](#).

6.4 Apple School Manager lehnt einen Upload ohne Schüler ab

Apple School Manager lehnt einen Upload ab, der keinen Schüler enthält, und zeigt einen Fehler an. Jedes Konto braucht mindestens einen Schüler in seinem Upload.

Ein Upload enthält in den folgenden Fällen keine Schüler:

- Keine der Schulen, die das Konto erhält, hat einen Schüler.
- Der LDAP-Filter für Schüler schließt alle Schüler dieser Schulen aus. Siehe [Benutzer mit einem LDAP-Filter auswählen](#).

Um den Fehler zu sehen, folgen Sie [Aussagekräftigere Fehlermeldungen von Apple School Manager erhalten](#).

6.5 Der Lauf bricht mit einem Fehler bei den Zugangsdaten ab

Der Connector bricht ab, bevor er Daten sammelt, wenn `/etc/asm-connections.json` fehlt oder ungültig ist oder wenn eine Passwortdatei fehlt oder leer ist. Die Meldung in der Logdatei nennt die Datei und den Eintrag.

Quellcode 6.3: Meldung in der Logdatei

```
No Apple School Manager account configured. Create /etc/asm-connections.json as
described in the Apple School Manager Connector manual.
```

Konfigurieren Sie die Konten, wie in [Konten in Apple School Manager](#) beschrieben. Wenn die Zugangsdaten gesetzt sind, Apple sie aber ablehnt, erzeugen Sie in Apple School Manager neue Zugangsdaten und tragen Sie diese ein.

6.6 Der Upload bricht mit einem fehlenden Host-Schlüssel ab

Der Connector prüft den Host-Schlüssel des SFTP-Servers gegen `/etc/asm_public_key`. Das Paket liefert diese Datei mit. Fehlt sie oder passt sie nicht mehr zum Server, schlägt der Upload mit `Could not find /etc/asm_public_key` oder mit einem SSH-Fehler fehl.

Installieren Sie das Paket erneut, um die Datei wiederherzustellen. Wenn Apple den Host-Schlüssel geändert hat, melden Sie dies Univention, siehe [Hilfe erhalten](#), damit eine neue Version der App den neuen Schlüssel mitliefern kann.

6.7 Der Upload in ein Konto bricht mit einem ungültigen LDAP-Filter ab

Ein LDAP-Filter mit einem Syntaxfehler bricht den Upload in das Konto dieser Schule ab. Der Connector lädt trotzdem in die übrigen Konten hoch und endet am Schluss mit einem Exit-Status ungleich null. Die Logdatei nennt den Filter und das Konto.

Quellcode 6.4: Meldungen in der Logdatei

```
Invalid LDAP-filter for students: '(ucsschoolRole=student'  
Invalid LDAP filter, nothing uploaded to account north.
```

Korrigieren Sie den Filter in der Einstellungsdatei oder entfernen Sie den Schlüssel `ldap_filter` der Schule, damit der Filter aus `defaults` greift. Siehe [Benutzer mit einem LDAP-Filter auswählen](#).

6.8 Klassen haben weniger Lehrer als erwartet

Apple School Manager unterstützt höchstens 15 Lehrer pro Klasse. Der Connector exportiert die ersten 15 und schreibt eine Warnung mit dem Namen der Klasse in die Logdatei. Das ist eine Einschränkung von Apple School Manager, nicht des Connectors.

Auch ein LDAP-Filter für Lehrer kann die Anzahl verringern. Die Logdatei verzeichnet jeden Lehrer, den ein Filter aus einer Klasse ausgeschlossen hat.

6.9 Die Föderation für eine Domain schlägt beim zweiten Mal fehl

Wenn Sie die Föderation für eine Domain deaktivieren und anschließend wieder aktivieren, zeigt Apple School Manager einen Fehler an.

Solange die Föderation aktiv ist, bietet Apple School Manager an, die Domain zu trennen, statt sie zu entfernen. Das Trennen nimmt die Domain nur aus der Föderation heraus. Die Domain selbst bleibt in Apple School Manager erhalten.

Um die Föderation für die Domain wieder zu aktivieren, gehen Sie wie folgt vor:

1. Trennen Sie in Apple School Manager die Verbindung zum Identity Provider.
2. Verbinden Sie ihn erneut, wie in [Identity Provider verbinden](#) beschrieben.
3. Aktivieren Sie die Föderation für die Domain, wie in [Föderation für die Domain aktivieren](#) beschrieben.

6.10 Hilfe erhalten

- Das Forum [Univention Help](#) für Fragen aus der Community.
- Ihr Univention-Supportvertrag für eine unterstützte Umgebung.

Wenn Sie ein Problem melden, hängen Sie den relevanten Ausschnitt aus `/var/log/univention/asm.log` an.

Dieses Kapitel listet die Änderungen jeder veröffentlichten Version der App auf.

7.1 v6.0.0 (2026-10-19)

- Der Connector synchronisiert in mehrere Konten in Apple School Manager. Jedes Konto erhält nur die Schulen, die Sie ihm zuordnen.
- Die Einstellungsdatei `/etc/asm-connections.json` ersetzt die App-Einstellungen `asm/username`, `asm/password` und `asm/school_whitelist` sowie alle UCR-Variablen `asm/attributes/*` und `asm/ldap_filter/*`. Die Einstellungen für Schüler und Lehrer gelten pro Konto, die Einstellungen für Klassen und die LDAP-Filter pro Schule. Das Update überträgt die bisherigen Werte in die neue Datei, wie in *Update von einer früheren Version* beschrieben.
- Ein Fehler beim Upload in ein Konto, zum Beispiel ein ungültiger LDAP-Filter, bricht nur den Upload in dieses Konto ab.
- `asm/last_upload/ACCOUNT` enthält den Zeitpunkt des letzten Uploads in jedes Konto.
- Der Connector prüft nicht mehr, ob sich die Domain einer E-Mail-Adresse auflösen lässt. Die Prüfung schrieb nur eine Warnung, und Apple School Manager akzeptiert solche Adressen.
- Die App unterstützt Keycloak als Identity Provider für Apple School Manager. Benutzer melden sich mit dem Passwort aus der UCS@school-Domäne an ihren Managed Apple Accounts an. Siehe *Keycloak als Identity Provider für ASM*.

7.2 v5.1.1 (2026-03-05)

- Der Connector lässt sich wieder auf einem zentralen Replica Directory Node betreiben.

7.3 v5.1.0

- Der Connector exportiert weitere zusätzliche Standorte für Schüler und Lehrer.

7.4 v5.0.3

- Die App verweigert die Installation auf einem zentralen Replica Directory Node.

7.5 v5.0.2

- Folge-Release für Version 5.0.1. Eine nicht passende Komponenten-ID im App Center verhinderte das Update von UCS 5.0.

7.6 v5.0.1

- Erstes Release für UCS@school 5.2. Funktional identisch mit Version 3.0.3.

7.7 v4.0.0

- Erstes Release für UCS@school 5.1. Funktional identisch mit Version 3.0.3.

7.8 v3.0.3

- Eine Debian-Abhängigkeit wurde korrigiert.

7.9 v3.0.2

- Der Connector exportiert die Jahrgangsstufe, die mit `asm/attributes/student/grade_level` konfiguriert wird.

7.10 v3.0.1

- Die Logrotation des Connectors folgt den UCR-Variablen `logrotate/*`.

7.11 v2.2.4

- Der Connector wendet konfigurierte LDAP-Filter beim Laden von Klassen korrekt an.

7.12 v2.2.3

- Die Behandlung unerwarteter Fehler wurde korrigiert.

7.13 v2.2.2

- Der Name eines Kurses, den der Connector aus der Schulklasse ableitet, folgt dem Muster in `asm/attributes/course-name-pattern`. Die Voreinstellung ist `{ou}-{name}`.

7.14 v2.2.1

- Der Connector wendet konfigurierte LDAP-Filter auf `rosters.csv` an.

7.15 v2.2.0

- Der Connector verwendet den Namen der Schulklasse als Kursnamen. Zuvor verwendete er die Beschreibung der Schulklasse.
- LDAP-Filter ermöglichen eine feinere Steuerung der exportierten Lehrer und Schüler. Sie lassen sich global oder pro Schule mit `asm/ldap_filter/students` und `asm/ldap_filter/staff` setzen. Ein ungültiger Filter bricht die Synchronisation ohne Export ab.

7.16 v2.1.0

- Der Connector füllt die Spalte `password_policy` für neue Schüler aus `asm/attributes/student/password_policy`.

7.17 v2.0.0

- Erstes Release für UCS 4.4. Funktional identisch mit Version 1.2.

7.18 v1.2.0

- Der Connector verarbeitet Klassen mit mehr als 15 Lehrern korrekt. Er exportiert 15 davon, was dem Limit von Apple School Manager entspricht.

7.19 v1.1.0

- Sie können die App auf einem Replica Directory Node installieren.

7.20 v1.0.0

- Erstes Release.

App Center

Das Univention App Center, die Komponente von *UCS*, mit der Sie Apps installieren und konfigurieren.

Apple School Manager

Der Webdienst, mit dem Bildungseinrichtungen ihre Managed Apple Accounts, Geräte und Inhalte verwalten. Abgekürzt als ASM.

Keycloak

Die Software für Identitäts- und Zugriffsverwaltung, die UCS als App bereitstellt. Sie liefert das Single Sign-On der Domäne.

OIDC

OpenID Connect, die Identitätsschicht auf Basis von OAuth 2.0.

PKCE

Proof Key for Code Exchange, eine Erweiterung des Authorization Code Flow von OAuth 2.0.

SSF

Shared Signals Framework, der Standard der OpenID Foundation für den Austausch von Sicherheitsereignissen zwischen einem Identity Provider und den Anwendungen, die sich auf ihn stützen.

UCR

Univention Configuration Registry, die zentrale Konfigurationsdatenbank von *UCS*.

UCS

Univention Corporate Server, das Server-Betriebssystem mit integriertem Identity Management.

UCS@school

Die Erweiterung von *UCS* für Schulen und Schulträger.

UMC

Univention Management Console, die Weboberfläche für die Administration von *UCS*.

KAPITEL 9

Literaturverzeichnis

Literaturverzeichnis

- [1] Univention GmbH. Univention Corporate Server 5.2 - Manual for users and administrators. URL: <https://docs.software-univention.de/manual/5.2/en/> (visited on 2026-10-08).
- [2] Univention GmbH. UCS@school - Handbuch für Administratoren. URL: <https://docs.software-univention.de/ucsschool-manual/5.2/de/> (visited on 2026-10-08).
- [3] Apple Inc. Upload apple formatted csv files in apple school manager. URL: <https://support.apple.com/en-us/101183> (visited on 2026-09-11).
- [4] Apple Inc. Create managed apple accounts with SFTP in apple school manager. URL: <https://support.apple.com/en-us/HT207029> (visited on 2026-09-11).
- [5] OpenID Foundation. Shared signals framework specification 1.0. URL: https://openid.net/specs/openid-sharedsignals-framework-1_0.html (visited on 2026-09-11).
- [6] Apple Inc. Add and verify a domain. URL: <https://support.apple.com/guide/apple-school-manager/add-and-verify-a-domain-axm48c3280c0/web> (visited on 2026-09-11).
- [7] Apple Inc. Intro to roles and privileges in apple school manager. URL: <https://support.apple.com/guide/apple-school-manager/intro-to-roles-and-privileges-axm97dd59159/web> (visited on 2026-10-02).
- [8] Apple Inc. Sign in and manage your apple account on iPhone. URL: <https://support.apple.com/guide/iphone/sign-in-and-manage-your-apple-account-iph76e54c61e/ios> (visited on 2026-09-11).

A

App Center, [31](#)

Apple School Manager, [31](#)

K

Keycloak, [31](#)

keycloak/server/feature/ssf, [18](#)

keycloak/server/sso/fqdn, [18](#)

O

OIDC, [31](#)

P

PKCE, [31](#)

S

SSF, [31](#)

U

UCR, [31](#)

UCS, [31](#)

UCS@school, [31](#)

UMC, [31](#)

Umgebungsvariable

keycloak/server/feature/ssf, [18](#)

keycloak/server/sso/fqdn, [18](#)