



Apple School Manager Connector Documentation

Release 6.0.0

Univention GmbH

Oct 23, 2026

The source of this document is licensed under [GNU Affero General Public License v3.0](#) only.

CONTENTS

1	Introduction	1
1.1	Who this documentation is for	1
1.2	What you need	1
1.3	What the connector synchronizes	1
1.4	Passwords and devices	2
2	Installation	3
2.1	Supported system roles	3
2.2	Install the app	3
2.3	Obtain the SFTP credentials	4
2.4	Enter the credentials	4
3	Configuration	5
3.1	Settings file	5
3.2	App settings	9
3.3	Schedule the synchronization	10
3.4	Settings in detail	10
4	Synchronization	13
4.1	Run the synchronization	13
4.2	The CSV files	14
4.3	Inspect the uploaded data	16
5	Keycloak as identity provider for ASM	17
5.1	Why Apple School Manager needs SSF	17
5.2	What you need	17
5.3	Configure Keycloak	18
5.4	Configure Apple School Manager	20
5.5	Sign in on a device	21
6	Troubleshooting	23
6.1	Log file	23
6.2	Get better error messages from Apple School Manager	23
6.3	Users don't appear in Apple School Manager	23
6.4	Apple School Manager rejects an upload without students	24
6.5	The run stops with a credential error	24
6.6	The upload stops with a missing host key	24
6.7	The upload to an account stops with an invalid LDAP filter	24
6.8	Classes have fewer teachers than expected	25
6.9	Federation for a domain fails the second time	25
6.10	Where to get help	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	27
7.5	v5.0.2	27
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	28
7.16	v2.1.0	28
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	Glossary	31
9	Bibliography	33
	Bibliography	35
	Index	37

INTRODUCTION

The *Apple School Manager Connector* is an app for *UCS@school*. It provisions the schools, classes, work groups, teachers, and students of your UCS@school domain to *Apple School Manager*, so that you don't have to maintain the same accounts twice.

In this setup, UCS@school takes the role of the student information system that Apple School Manager expects, and the connector uses the SFTP interface that Apple provides for such systems. The connector collects the data from the LDAP directory, writes it to a set of CSV files, packs them into a ZIP archive, and uploads that archive to Apple School Manager.

1.1 Who this documentation is for

This documentation addresses administrators who run a UCS@school domain and who want to provision its users to Apple School Manager. It assumes that you're familiar with the administration of *UCS* and UCS@school, in particular with the following topics:

- The *App Center*, see *Univention App Center* in the UCS manual [1].
- The *UCR*, see *Administration of local system configuration with Univention Configuration Registry* in the UCS manual [1].
- The school objects that UCS@school manages, see *UCS@school-Objekte im LDAP-Verzeichnisdienst* in the UCS@school manual [2], which is available only in German.

1.2 What you need

Before you start, make sure that you have the following:

- A UCS@school domain with at least one school.
- An Apple School Manager account for an educational institution.
- The SFTP credentials for the Apple School Manager account. *Obtain the SFTP credentials* describes where to find them.
- A primary email address for each user. Apple School Manager uses the email address as the Apple Account and can't create an account for a user without one.

1.3 What the connector synchronizes

The connector transfers data in one direction only, from UCS@school to Apple School Manager. It never reads data back, and it never changes objects in your UCS@school domain.

The following table lists what the connector maps to which Apple School Manager entity.

Table 1.1: Objects that the connector synchronizes

UCS@school object	Apple School Manager entity
School	Location
School class or work group	Course and class
Student	Student
Teacher and teacher with staff role	Staff member
Membership of a student in a school class or work group	Roster entry

Apple School Manager requires every class to belong to a course, so the connector turns each school class and work group into a course with exactly one class in it. See [Courses](#).

Staff members without a teacher role aren't synchronized. Exam users aren't synchronized either.

[Synchronization](#) describes the mapping in detail, including the individual CSV columns.

1.4 Passwords and devices

The connector never transfers passwords. Apple School Manager creates the passwords for new accounts itself, and you distribute them from there. [Password policy for students](#) describes how to influence the length of those passwords.

For device management, Univention recommends a mobile device management solution that offers an interface to Apple School Manager. The [Univention integration catalog](#) lists the solutions that integrate with UCS@school.

INSTALLATION

You install the *Apple School Manager Connector* from the [App Center](#), like any other app. This chapter describes where you can install it, how to install it, and how to obtain the credentials that the connector needs.

2.1 Supported system roles

You can install the connector on the following system roles:

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

Caution

Install the connector on exactly one system in the domain.

Every installation uploads a complete data set and overwrites what the previous upload transferred. Two installations therefore overwrite each other's data. If you want to synchronize additional schools, add them to the existing installation as described in [Schools](#), or add another Apple School Manager account as described in [Apple School Manager accounts](#).

On a school Replica Directory Node, the connector only sees the school of that node. On a central Replica Directory Node, a Primary Directory Node, or a Backup Directory Node, it sees every school in the domain.

2.2 Install the app

1. Open the App Center in [UMC](#).
2. Select *Apple School Manager Connector*.
3. Click *Install*.

After the installation, obtain the credentials as described in the next section and enter them as described in [Enter the credentials](#).

Note

The connector requires UCS@school in version 5.2v5 or later. The app refuses to update on a system with an older version.

2.3 Obtain the SFTP credentials

Apple School Manager generates the SFTP user name and password for you. To find them, do the following:

1. Sign in to [Apple School Manager](#).
2. Click your name in the lower-left corner and select *Preferences*.
3. Select *Managed Apple Accounts*.
4. Open the menu for *Apple formatted CSV*.
5. Click *Upload CSV*.

A new frame opens and shows the SFTP account data. For background information, see Apple Inc. [3].

2.4 Enter the credentials

1. Store the password in `/etc/asm.secret` with read permission for the `root` user only.

Listing 2.1: Store the password

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

2. Add the user name, the path of the password file, and the schools to the settings file `/etc/asm-connections.json`, which the installation creates without an account.

Listing 2.2: One Apple School Manager account in `/etc/asm-connections.json`

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

The entry `*` in `schools` synchronizes every school to the account.

[Settings file](#) describes the file in detail, including how to limit the account to individual schools, how to add further accounts, and every setting for users and classes. Then continue with [Configuration](#).

CONFIGURATION

The connector reads its configuration from two places. The settings file `/etc/asm-connections.json` holds the Apple School Manager accounts, the schools that the connector synchronizes to each of them, and every setting that controls which users the connector exports and how it maps their attributes. The app settings in the *App Center* hold the synchronization schedule and a few switches for everyday operation.

Caution

Apple School Manager uses the email address of a user as the Apple Account. Make sure that every synchronized user has a primary email address. Apple School Manager can't create an account for a user without one. See *Email addresses*.

3.1 Settings file

The settings file `/etc/asm-connections.json` has three sections:

accounts

The Apple School Manager accounts, each with its credentials and the settings for the students and teachers that the account receives. See *Apple School Manager accounts*.

schools

The schools to synchronize, each with the account that receives it and the settings for its classes. See *Schools*.

defaults

Settings that apply to every account and every school, unless an account or a school entry sets them itself. See *Defaults*.

Listing 3.1: Two Apple School Manager accounts in `/etc/asm-connections.json`

```
{
  "accounts": {
    "north": {
      "username": "sftp-user-north",
      "password_file": "/etc/asm-north.secret"
    },
    "south": {
      "username": "sftp-user-south",
      "password_file": "/etc/asm-south.secret",
      "student": {"anonymize": false}
    }
  },
  "defaults": {
    "student": {"password_policy": 6}
  },
  "schools": {
```

(continues on next page)

(continued from previous page)

```

    "gym123": {"account": "north"},
    "gs456": {
        "account": "south",
        "course_name_pattern": "{name}",
        "student": {"ldap_filter": "(uid=a*)"}
    }
}

```

A student or teacher who belongs to several schools of the same account appears only once in the upload to that account. The settings for students and teachers therefore apply per account, and the settings for classes and the LDAP filters apply per school.

For every setting, the connector uses the value from the account or school entry, then the value from `defaults`, and then the built-in default.

The installation creates the file with read permission for the `root` user only. Edit it with a text editor. The connector reads the file at the start of each run, so a change takes effect with the next synchronization. It checks the complete file before it uploads anything. The following problems stop the run with an error message that names the file and the entry:

- A missing file, or a file without an account or a school.
- A missing or unknown key, or a value of the wrong type.
- A school that refers to an account that the file doesn't define.
- A missing or empty password file.
- A user name that appears for more than one account.
- A school that doesn't exist, if the file has the entry `*`. A misspelled school would otherwise send its users to the account of that entry.
- No account that receives an existing school.

The following problems only write a warning to the log file. The connector uploads to the remaining accounts:

- An account that no school refers to. The account receives no upload.
- A school that doesn't exist, if the file has no entry `*`. An account without any existing school receives no upload.

If the upload to one account fails, the connector still uploads to the remaining accounts and exits with a non-zero status at the end.

3.1.1 Apple School Manager accounts

The `accounts` section maps a name of your choice to each account. The name may only contain letters, digits, `.`, `_`, and `-`. Usually there is a single account. If the schools on your UCS@school system belong to different institutions, each with its own Apple School Manager account, add one entry per account. The connector then uploads a separate archive to every account, each restricted to the schools that refer to that account.

To add an account:

1. Store the SFTP password of the account in a file of its own that only `root` can read. *Obtain the SFTP credentials* describes where to find the password. Every account has its own SFTP credentials, so every account needs its own password file. The examples name the file after the account, such as `/etc/asm-north.secret`. The account from *Enter the credentials* can keep `/etc/asm.secret`.

Listing 3.2: Store the password of an account

```

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

```

2. Add the account to the `accounts` section of the settings file.

3. Assign at least one school to the account, as described in [Schools](#).

An account entry takes the following keys. All keys except `username` and `password_file` are optional and can also go to defaults.

Table 3.1: Keys of an account entry

Key	Default	Description
<code>username</code>	Required	The SFTP user name of the account.
<code>password_file</code>	Required	Path to the file that holds the SFTP password of the account.
<code>email_prepend_domain</code>	Empty	See Email addresses .
<code>student.anonymize,</code> <code>staff.anonymize</code>	<code>true</code>	See Anonymization .
<code>student.anonymize_values,</code> <code>staff.anonymize_values</code>	See Anonymization	See Anonymization .
<code>student.</code> <code>person_id_attribute,</code> <code>staff.</code> <code>person_id_attribute</code>	<code>entryUUID</code>	See Identification of users .
<code>student.password_policy</code>	<code>4</code>	See Password policy for students .
<code>student.</code> <code>grade_level_attribute</code>	<code>null</code>	See Grade level of students .

3.1.2 Schools

The `schools` section lists the schools to synchronize by their abbreviation and assigns each of them to an account. The connector only synchronizes schools that the section lists.

To look up the abbreviations, open *School administration* ▶ *Schools* in *UMC*. The abbreviation is the name of the school object, for example `gym123`.

The entry `*` stands for every school that the section doesn't list by name. With a single account, it synchronizes all schools to that account.

If the section lists a school that doesn't exist, the connector stops before it uploads anything. Otherwise a misspelled school would go to the account of the entry `*` instead of the account you meant.

Listing 3.3: Every school to one account, one school with its own LDAP filter

```
"schools": {
  "*": {"account": "north"},
  "gym123": {
    "account": "north",
    "staff": {"ldap_filter": "(uid=t*)"}
  }
}
```

A student or teacher who belongs to several schools appears in the upload to an account only with the schools that belong to that account. If none of their schools belongs to the account, the connector skips them for that account.

A school entry takes the following keys. All keys except `account` are optional and can also go to `defaults`.

Table 3.2: Keys of a school entry

Key	Default	Description
<code>account</code>	Required	Name of the account in the <code>accounts</code> section that receives the school.
<code>course_name_pattern</code>	<code>{ou}-{name}</code>	See <i>Names of courses and classes</i> .
<code>class_number_empty</code>	<code>true</code>	See <i>Names of courses and classes</i> .
<code>student.ldap_filter</code> , <code>staff.ldap_filter</code>	Empty	See <i>Select users with an LDAP filter</i> .

3.1.3 Defaults

The `defaults` section takes every optional key of an account entry and of a school entry. A value in `defaults` applies to every account or every school that doesn't set the key itself.

Listing 3.4: Anonymize nobody, except the students of the account `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 from an earlier version

Up to version 5.1.1, app settings and UCR variables held the configuration. The update to version 6.0.0 moves their values to the settings file and removes the UCR variables. You don't need to do anything. The password stays in `/etc/asm.secret`, and the settings file refers to it. The account gets the name `default`.

Table 3.3: Former app settings and UCR variables

Former setting	Key in the settings file	
asm/username	accounts.default.username	
asm/password	accounts.default.password_file	
asm/school_whitelist	One entry per school in schools, or the entry * if the list was empty	
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, without the leading %	
asm/attributes/student/password_policy	defaults.student.password_policy, null for the former –	
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

Replace `ROLE` with `staff` or `student`, `ATTRIBUTE` with an attribute from [Anonymization](#), and `SCHOOL` with the school abbreviation.

The update drops an LDAP filter for a school that wasn't on the former school list, because the connector didn't synchronize that school. It also leaves out schools that don't exist any more, both from the former school list and from the LDAP filters, and prints a note for each of them.

Without `asm/username`, the update has no account to assign schools to. It keeps `asm/school_whitelist` and the `asm/ldap_filter/students/SCHOOL` and `asm/ldap_filter/staff/SCHOOL` UCR variables and prints a note for each of them. Move their values to the settings file when you add the account.

If `/etc/asm-connections.json` already exists, the update leaves it and the UCR variables unchanged.

3.2 App settings

To open the app settings, select the app in the App Center and click *App settings*. The app settings apply to every account alike.

Table 3.4: App settings of the Apple School Manager Connector

Setting	Default	Description
asm/sync_daily	False	Run the synchronization once a day. See Schedule the synchronization .
asm/sync_daily/hour	Unset	The hour of the day at which the daily synchronization runs. Valid values are 0 to 23.
asm/ run_on_appsetting_save	False	Run the synchronization immediately after you save the app settings.
asm/store_zip	False	Keep the uploaded ZIP archive in <code>/var/lib/asm/</code> instead of deleting it after the upload.
asm/last_upload	Unset	Read-only status field. Shows when the connector last uploaded an archive to any account.
asm/last_upload/ ACCOUNT	Unset	Shows when the connector last uploaded an archive to the account <code>ACCOUNT</code> . Not part of the app settings.

3.3 Schedule the synchronization

The connector doesn't run on its own. Either you run it manually, as described in [Run the synchronization](#), or you let a cron job run it once a day.

To enable the daily run:

1. Open the app settings.
2. Select *asm/sync_daily*.
3. Select the hour in *asm/sync_daily/hour*.
4. Click *Apply changes*.

The connector writes the cron job to `/etc/cron.d/asm-upload`. The job runs at minute 0 of the selected hour. If you enable the daily run without a valid hour, the connector writes a comment to the cron file instead of a job, and no synchronization takes place.

3.4 Settings in detail

The following sections describe the optional keys of the settings file. Keys that start with `student` or `staff` go into an object of that name, as in `"student": {"anonymize": false}`.

3.4.1 Email addresses

Apple School Manager uses the email address of a user as the Apple Account. The connector exports the primary email address of each user in `UCS@school`. Users without one are exported without an email address, and Apple School Manager can't create an Apple Account for them.

email_prepend_domain

Per account. Inserts the value as a subdomain in front of the domain of every email address. With the value `apple`, the connector exports the address `jane@example.com` as `jane@apple.example.com`. Default: empty.

3.4.2 Anonymization

If you don't want to transfer the names and email addresses of your users, you can anonymize them. Anonymization replaces the values of the attributes `first_name`, `middle_name`, `last_name`, `email_address`, and `sis_user_name` with values that you configure.

Caution

An anonymized user has no email address, unless you configure a replacement value for it. Without an email address, Apple School Manager can't create an Apple Account for the user.

Anonymization and the [Keycloak as identity provider for ASM](#) setup exclude each other. If you use Keycloak as an identity provider for Apple School Manager, turn anonymization off.

student.anonymize, staff.anonymize

Per account. Enables anonymization for students and teachers. Default: `true`.

student.anonymize_values, staff.anonymize_values

Per account. Replacement values for the anonymized attributes. A value that starts with `%` names an LDAP attribute, and the connector exports the value of that attribute from the user's LDAP object. A value without a leading `%` is exported literally. `null` leaves the column empty. You only need to list the attributes whose default you want to change.

Table 3.5: Replacement values for anonymized attributes

Key in <code>anonymize_values</code>	Default	Required
<code>first_name</code>	<code>%uid</code>	Yes
<code>middle_name</code>	<code>null</code>	No
<code>last_name</code>	<code>-</code>	Yes
<code>email_address</code>	<code>null</code>	No
<code>sis_username</code>	<code>%uid</code>	No

Listing 3.5: Anonymize students with a fixed last name

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

3.4.3 Identification of users

Apple School Manager identifies a user by the `person_id` column. The connector fills it with an LDAP attribute of the user that doesn't change when you rename the user.

`student.person_id_attribute`, `staff.person_id_attribute`

Per account. LDAP attribute that identifies a student or a teacher. Default: `entryUUID`.

Caution

Don't change these keys on a running installation. Apple School Manager treats a user with a new `person_id` as a different user and loses the association with the existing account.

3.4.4 Password policy for students

Apple School Manager creates the password for a new student itself. The password policy determines how long that password is.

`student.password_policy`

Per account. Length of the password that Apple creates for a new student. Valid values are 4, 6, 8, and `null`. `null` means that Apple School Manager uses the default of the school. Default: 4.

Apple School Manager doesn't support a password policy for teachers.

3.4.5 Grade level of students

`student.grade_level_attribute`

Per account. LDAP attribute that holds the grade level of a student. The connector exports its value in the `grade_level` column. Default: `null`, which leaves the column empty.

3.4.6 Names of courses and classes

UCS@school prefixes the name of a school class with the school abbreviation, for example `gym123-1a`. The connector derives the course name from that name.

`course_name_pattern`

Per school. Pattern for the course name. The connector replaces `{ou}` with the school abbreviation and `{name}` with the class name without the school prefix. Default: `{ou}-{name}`.

`class_number_empty`

Per school. Leaves the `class_number` column empty. Apple School Manager builds the name of a class from

the course name and the class number, so an identical class number only repeats the course name. Default: `true`.

3.4.7 Select users with an LDAP filter

If the school list from *Schools* isn't fine-grained enough, you can select the users with an LDAP filter. The connector applies the filter in addition to the school list.

`student.ldap_filter`, `staff.ldap_filter`

Per school. LDAP filter for the students or the teachers of the school. A filter in `defaults` applies to every school that doesn't set its own. Default: empty, which selects every user.

Listing 3.6: Synchronize only the students of `gym123` with a primary email address

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

The connector combines the filter with its own selection of the students or teachers of the school, so the filter only needs to describe the attributes of the users you want. To check which users a filter selects before you set it, combine it with the role of the users and run it with `univention-ldapsearch`:

Listing 3.7: List the students of `gym123` who match the filter

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

Caution

An invalid LDAP filter stops the upload to the account of that school. The connector uploads nothing to that account in that case, so its data in Apple School Manager stays as it was after the last successful run. The other accounts still receive their upload.

SYNCHRONIZATION

A synchronization run reads the school data from the LDAP directory, writes it to CSV files, packs the files into a ZIP archive, and uploads the archive to Apple School Manager. This chapter describes the run itself and the data that it transfers.

4.1 Run the synchronization

Three things start a synchronization run:

- The cron job from *Schedule the synchronization*.
- Saving the app settings, if you enabled `asm/run_on_appsetting_save`.
- The command **asm-upload** on the command line.

Listing 4.1: Start a synchronization run manually

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

The command writes progress messages to the terminal and a more detailed log to `/var/log/univention/asm.log`. It exits with a non-zero status if the credentials are missing or if the upload to any account fails.

4.1.1 What happens during a run

1. The connector reads the settings file `/etc/asm-connections.json`, as described in *Settings file*. A missing or invalid entry stops the run, and so does a school that doesn't exist in the LDAP directory.
2. The connector collects the schools, classes, work groups, teachers, and students from the LDAP directory, restricted to the schools of the account and by the LDAP filters from *Select users with an LDAP filter*.
3. The connector writes the six CSV files from *The CSV files* to a temporary directory.
4. The connector packs the CSV files into `/var/lib/asm/asm_TIMESTAMP.zip` and removes the temporary directory. `TIMESTAMP` is the time the connector created the archive, in ISO 8601 format, for example `2026-10-01T03:00:12.345678`.
5. The connector opens an SFTP connection to `upload.appleschoolcontent.com` and uploads the archive as `archive.zip`. It verifies the host key against `/etc/asm_public_key`.
6. The connector sets `asm/last_upload` and `asm/last_upload/ACCOUNT` to the current time and deletes the archive, unless you enabled `asm/store_zip`.

With several accounts, the connector repeats the steps 2 to 6 for each account.

Every run transfers the complete data set. The connector doesn't track what changed since the last run.

4.1.2 How Apple School Manager applies the data

Apple School Manager compares the uploaded data with the accounts that it holds:

- A user who appears for the first time gets a new account.
- A user who is no longer in the upload is deactivated immediately and deleted after 30 days.
- A user whose attributes changed keeps the account, as long as the `person_id` column is unchanged. See *Identification of users*.

4.2 The CSV files

The archive contains the following six files. Apple documents their format in Apple Inc. [4]. The connector sorts the rows of each file by school and then by user or class name.

Table 4.1: Files in the uploaded archive

File	Content
<code>locations.csv</code>	One row per school.
<code>courses.csv</code>	One row per school class and work group.
<code>classes.csv</code>	One row per school class and work group, with the teachers of that class.
<code>staff.csv</code>	One row per teacher.
<code>students.csv</code>	One row per student.
<code>rosters.csv</code>	One row per membership of a student in a school class or work group.

4.2.1 Locations

Table 4.2: Columns of `locations.csv`

Column	Source in UCS@school
<code>location_id</code>	Name of the school, for example <code>gym123</code> .
<code>location_name</code>	Display name of the school. Falls back to the name if the school has no display name.

4.2.2 Courses

Apple School Manager requires every class to belong to a course. UCS@school only has the school class or work group, so the connector exports each of them twice: once as a course in `courses.csv` and once as a class of that course in `classes.csv`. Both rows use the name of the group as their ID, so each course has exactly one class.

Table 4.3: Columns of `courses.csv`

Column	Source in UCS@school
<code>course_id</code>	Name of the school class or work group, including the school prefix, for example <code>gym123-1a</code> .
<code>course_number</code>	Same value as <code>course_id</code> .
<code>course_name</code>	Built from <code>course_name_pattern</code> . See <i>Names of courses and classes</i> .
<code>location_id</code>	Name of the school.

4.2.3 Classes

Table 4.4: Columns of `classes.csv`

Column	Source in UCS@school
<code>class_id</code>	Name of the school class or work group.
<code>class_number</code>	Empty by default. See <code>class_number_empty</code> in <i>Names of courses and classes</i> .
<code>course_id</code>	Name of the school class or work group.
<code>instructor_id</code> , <code>instructor_id_2</code> , <code>instructor_id_3</code>	The <code>person_id</code> of the first three teachers of the class.
<code>instructor_id_4</code> to <code>instructor_id_15</code>	The <code>person_id</code> of the remaining teachers. The connector only writes as many columns as it needs.
<code>location_id</code>	Name of the school.

Note

Apple School Manager supports at most 15 teachers per class. If a class has more, the connector synchronizes the first 15 and writes a warning to the log file.

4.2.4 Staff

Table 4.5: Columns of `staff.csv`

Column	Source in UCS@school
<code>person_id</code>	The attribute from <code>staff.person_id_attribute</code> , <code>entryUUID</code> by default.
<code>person_number</code>	Same value as <code>person_id</code> .
<code>first_name</code>	First name of the teacher.
<code>middle_name</code>	First value of <code>middleName</code> , <code>initials</code> , or <code>oxMiddleName</code> .
<code>last_name</code>	Last name of the teacher.
<code>email_address</code>	Primary email address, modified by <code>email_prepend_domain</code> .
<code>sis_username</code>	User name of the teacher.
<code>location_id</code>	Primary school of the teacher.
<code>location_id_2</code> and following	The other schools of the teacher, in alphabetical order.

The file holds teachers and teachers with an additional staff role. Staff members without a teacher role aren't part of the export.

4.2.5 Students

Table 4.6: Columns of `students.csv`

Column	Source in UCS@school
<code>person_id</code>	The attribute from <code>student.person_id_attribute</code> , entryUUID by default.
<code>person_number</code>	Same value as <code>person_id</code> .
<code>first_name</code>	First name of the student.
<code>middle_name</code>	First value of <code>middleName</code> , <code>initials</code> , or <code>oxMiddleName</code> .
<code>last_name</code>	Last name of the student.
<code>grade_level</code>	The attribute from <code>student.grade_level_attribute</code> . Empty if the key is unset.
<code>email_address</code>	Primary email address, modified by <code>email_prepend_domain</code> .
<code>sis_username</code>	User name of the student.
<code>password_policy</code>	The value of <code>student.password_policy</code> . See <i>Password policy for students</i> .
<code>location_id</code>	Primary school of the student.
<code>location_id_2</code> and following	The other schools of the student, in alphabetical order.

Exam users aren't part of the export.

4.2.6 Rosters

Table 4.7: Columns of `rosters.csv`

Column	Source in UCS@school
<code>roster_id</code>	The class name and the <code>person_id</code> of the student, joined with a hyphen.
<code>class_id</code>	Name of the school class or work group.
<code>student_id</code>	The <code>person_id</code> of the student.

The file only holds students. Teachers reach a class through the `instructor_id` columns of `classes.csv`.

4.3 Inspect the uploaded data

To look at what the connector uploads, enable `asm/store_zip` in the app settings and run the synchronization. The connector then keeps the archive in `/var/lib/asm/`.

Listing 4.2: List the archives and unpack the newest one

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

Caution

The archives contain personal data. Delete them when you no longer need them, and turn `asm/store_zip` off again.

KEYCLOAK AS IDENTITY PROVIDER FOR ASM

Apple School Manager can federate the sign-in of its Managed Apple Accounts to an external identity provider. Your users then sign in to their Apple devices with the password from your UCS@school domain instead of a password that Apple School Manager manages.

This chapter describes how to set up the *Keycloak* app of *UCS* as that identity provider.

Caution

The *SSF* support that Apple School Manager requires is an experimental feature of Keycloak.

5.1 Why Apple School Manager needs SSF

The Shared Signals Framework is the standard of the OpenID Foundation for sharing security events, state changes, and risk signals between an identity provider and the applications that rely on it. See OpenID Foundation [5].

Apple School Manager uses SSF to learn about events in your domain, such as a changed credential or a revoked session. It therefore only accepts an identity provider that acts as an SSF transmitter. A plain *OIDC* client isn't enough.

5.2 What you need

- A UCS@school domain with the Apple School Manager Connector and the Keycloak app in version 26.7.2-nubus1 or later.
- A domain that you verified in Apple School Manager. See Apple Inc. [6]. Your users need a primary email address in that domain to sign in.
- An account in Apple School Manager with the *Administrator* role to connect the identity provider. See Apple Inc. [7]. This account can't sign in through the federation itself.
- An Apple device for the first sign-in.
- Anonymization turned off, because Apple School Manager needs the email address as the Apple Account:

Listing 5.1: Turn anonymization off in `/etc/asm-connections.json`

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

See *Anonymization*.

5.3 Configure Keycloak

Make every setting in the Keycloak admin console in the realm `ucs`, which holds the users of your domain. The admin console opens in the realm `master`. Select `ucs` in the realm selector before you change anything, and check the selected realm whenever you return to the admin console.

5.3.1 Enable the SSF feature

Set the app setting `keycloak/server/feature/ssf` of the Keycloak app to `true`.

1. Open the App Center in [UMC](#) and select the Keycloak app.
2. Click *App settings*.
3. Select `keycloak/server/feature/ssf`.
4. Click *Apply changes*.

Alternatively, set it on the command line:

Listing 5.2: Enable the SSF feature of Keycloak

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

The App Center then recreates the Keycloak container, which starts Keycloak with the SSF feature. Keycloak is unavailable for a short time while that happens.

Note

If you set the variable with `ucr set` instead, apply it with `univention-app configure keycloak`. Restarting the app with `univention-app restart keycloak` isn't enough, and the *Realm settings* page doesn't offer *SSF Transmitter*.

5.3.2 Turn the realm into an SSF transmitter

1. Open the Keycloak admin console at `https://ucs-sso-ng.DOMAIN/admin/` and select the realm `ucs`. Replace `DOMAIN` with the domain name of your UCS domain.
2. On the *Realm settings* page, set *SSF Transmitter* to *On*.

With the transmitter on, the realm offers an SSF configuration metadata endpoint next to the OpenID endpoint configuration. You need the URLs of both endpoints in [Connect the identity provider](#):

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

The URLs use the defaults of the Keycloak app: the host `ucs-sso-ng.DOMAIN` and the realm `ucs`, which holds the users of the domain. If you changed `keycloak/server/sso/fqdn` or use another realm, adjust the URLs accordingly.

5.3.3 Create the client scopes

On the realm's *Client scopes* page, create the client scopes `ssf.manage` and `ssf.read`, each with *Include in token scope* enabled.

5.3.4 Create the OIDC client

1. On the realm's *Clients* page, click *Create client*.
2. On the *General settings* page, enter `apple-asm` as *Client ID*.

- On the *Capability config* page, enter the settings from the following table.

Table 5.1: Capabilities of the OIDC client for Apple School Manager

Setting	Value
<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 doesn't appear to support [PKCE](#) for OIDC federations, which is why the client turns it off. The page doesn't offer *SSF Receiver* until *Client authentication* is on and you completed [Enable the SSF feature](#) and [Turn the realm into an SSF transmitter](#).

- On the *Login settings* page, enter the settings from the following table and click *Save*.

Table 5.2: Login settings of the OIDC client for Apple School Manager

Setting	Value
<i>Valid redirect URIs</i>	<code>https://gsa-ws.apple.com/grandslam/GsService2/acs</code>
<i>Valid post logout redirect URIs</i>	<code>+</code>

Copy the client secret from the *Credentials* tab. You need it in [Connect the identity provider](#).

5.3.5 Configure the client as an SSF receiver

- On the client's *Client scopes* tab, add `ssf.manage`, `ssf.read`, and `offline_access` as *Default*.
- On the *Roles* tab, add the client role `ssf-admin`.
- On the *SSF* tab, enter the settings from the following table.

Table 5.3: SSF settings of the client

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

Auto verify stream sends the verification event as soon as Apple creates the stream. *Emit-only events* lets you control through the Keycloak API when Keycloak sends a sign-out to Apple.

5.3.6 Create the administrative user

Apple School Manager establishes the connection to Keycloak with the authorization code flow. The resulting access token and refresh token belong to an offline session of one user, so that user must exist before you connect the two systems.

Create the user in Keycloak, not in UCS. Keycloak has only read access to the UCS users, so it can't assign client roles to them.

1. In the realm `ucs`, create a user, for example `asm`.
2. Set the first name, the last name, and the email address.
3. On the *Credentials* tab, set a strong password. Two-factor authentication is optional but recommended.
4. Assign the client role `ssf-admin` of the client `apple-asm`.

5.4 Configure Apple School Manager

5.4.1 Connect the identity provider

1. Sign in to [Apple School Manager](#).
2. Open *Preferences* ▶ *Managed Apple Accounts*.
3. Make sure that your domain is verified.
4. Under *User sign-in and directory sync*, click *Configure*. If another identity provider is connected, disconnect it first.
5. Select *Custom Identity Provider* and click *Continue*.
6. Enter a name for the identity provider, for example `asmkc`.
7. Enter the client ID and the client secret from [Create the OIDC client](#), and the two URLs from [Turn the realm into an SSF transmitter](#), as listed in the following table.

Table 5.4: Settings of the custom identity provider in Apple School Manager

Field	Value
<i>Client ID</i>	<code>apple-asm</code>
<i>Client Secret</i>	The client secret from the <i>Credentials</i> tab of the client
<i>SSF URL</i>	<code>https://ucs-sso-ng.DOMAIN/realms/ucs/.well-known/ssf-configuration</code>
<i>OIDC URL</i>	<code>https://ucs-sso-ng.DOMAIN/realms/ucs/.well-known/openid-configuration</code>

8. Click *Continue*.
9. In the window that opens, click the sign-in button for your identity provider, for example *Sign in with asmkc*.
10. Sign in with the administrative user from [Create the administrative user](#).

Apple School Manager shows *Authorizing Account* and then confirms the connection. During the connection, Apple creates an SSF stream for the client, which you can see on the client's *SSF Streams* tab in Keycloak.

5.4.2 Enable federation for the domain

1. Open *Preferences* ▶ *Managed Apple Accounts*.
2. Select your domain and click *Manage*.
3. At the bottom of the page, find the section for your identity provider and click *Set up*.
4. Switch the toggle that appears to *On*.
5. If the SFTP upload uses the domain, Apple School Manager asks you to choose another domain for the upload. Choose any other domain.

Apple School Manager enables federation for the domain and sends a confirmation email.

After that, every Managed Apple Account with an email address in the domain signs in through Keycloak. This includes accounts that existed before you enabled federation and accounts that you created manually in Apple School Manager.

The upload from the connector continues to work. Apple School Manager assigns the accounts by the domain of their email address, so the accounts from the upload belong to the federated domain, regardless of the domain that you chose for the SFTP upload.

5.5 Sign in on a device

After you enable federation for the domain, your users sign in to an Apple device with their UCS@school credentials. The following steps describe an unpaired device. See Apple Inc. [8] for the general procedure.

1. Open *Settings* ▶ *Apple Account*.
2. Tap *Sign In Manually*.
3. Enter the email address of the user in the federated domain and tap *Proceed*.
4. The device shows a hint that names your organization. Tap *Proceed*.
5. The Keycloak sign-in page opens with the user name already filled in. Enter the password.
6. Enter the device PIN when the device asks for it.

After the sign-in, *Settings* ▶ *Apple Account* shows the user with the email address from UCS@school.

TROUBLESHOOTING

This chapter describes where the connector records what it does and what to do about the problems that occur most often.

6.1 Log file

The connector writes to `/var/log/univention/asm.log`. The file holds the debug-level log of every run, including the teachers whom an LDAP filter excluded from a class. The app settings show the time of the last upload in `asm/last_upload`. `asm/last_upload/ACCOUNT` holds the time of the last upload to each account.

The log rotation follows the `logrotate/*` UCR variables of the system. The connector writes its own configuration to `/etc/logrotate.d/asm`.

Listing 6.1: Follow a synchronization run

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

6.2 Get better error messages from Apple School Manager

Apple School Manager reports errors in the uploaded data sparsely. The page that shows the SFTP credentials gives more details about the data that Apple School Manager rejects. You can keep the SFTP upload connected.

1. Open the page with the SFTP credentials, as described in [Obtain the SFTP credentials](#).
2. Keep the page open and start a synchronization run, as described in [Run the synchronization](#).

The page shows the errors of each upload while the upload runs.

6.3 Users don't appear in Apple School Manager

Check the following, in this order:

1. **The user has no primary email address.** The connector exports the user without an email address, and Apple School Manager can't create an Apple Account for the user.
2. **Anonymization removed the email address.** Anonymization is enabled by default. With `student.anonymize` or `staff.anonymize` enabled for the account, the connector exports the replacement value instead of the address, which is empty by default. See [Anonymization](#).

Listing 6.2: Turn anonymization off in `/etc/asm-connections.json`

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

3. **The school isn't on the list.** The connector only exports schools that the `schools` section of the settings file lists, and only to the account that the school refers to. See [Schools](#).
4. **An LDAP filter excludes the user.** The log file doesn't name users whom a filter excluded. Run the filter with `univention-ldapsearch` to check which users it selects. See [Select users with an LDAP filter](#).

6.4 Apple School Manager rejects an upload without students

Apple School Manager rejects an upload that contains no student and shows an error. Every account needs at least one student in its upload.

An upload contains no students in the following cases:

- None of the schools that the account receives has a student.
- The LDAP filter for students excludes every student of those schools. See [Select users with an LDAP filter](#).

To see the error, follow [Get better error messages from Apple School Manager](#).

6.5 The run stops with a credential error

The connector stops before it collects any data if `/etc/asm-connections.json` is missing or invalid, or if a password file is missing or empty. The message in the log file names the file and the entry.

Listing 6.3: Message in the log file

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

Configure the accounts, as described in [Apple School Manager accounts](#). If the credentials are set but Apple rejects them, generate new ones in Apple School Manager and enter those.

6.6 The upload stops with a missing host key

The connector verifies the host key of the SFTP server against `/etc/asm_public_key`. The package ships that file. If it's missing or no longer matches the server, the upload fails with `Could not find /etc/asm_public_key` or with an SSH exception.

Reinstall the package to restore the file. If Apple changed the host key, report it to Univention, see [Where to get help](#), so that a new version of the app can ship the new key.

6.7 The upload to an account stops with an invalid LDAP filter

An LDAP filter with a syntax error stops the upload to the account of that school. The connector still uploads to the remaining accounts and exits with a non-zero status at the end. The log file names the filter and the account.

Listing 6.4: Messages in the log file

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

Correct the filter in the settings file, or remove the `ldap_filter` key of the school to fall back to the filter in defaults. See *Select users with an LDAP filter*.

6.8 Classes have fewer teachers than expected

Apple School Manager supports at most 15 teachers per class. The connector exports the first 15 and writes a warning to the log file that names the class. This is a limitation of Apple School Manager, not of the connector.

An LDAP filter for teachers can also reduce the number. The log file records every teacher whom a filter excluded from a class.

6.9 Federation for a domain fails the second time

If you disable federation for a domain and then enable it again, Apple School Manager shows an error.

While federation is on, Apple School Manager offers to disconnect the domain instead of removing it. Disconnecting removes the domain only from the federation. The domain itself stays in Apple School Manager.

To enable federation for the domain again, do the following:

1. In Apple School Manager, disconnect the identity provider.
2. Connect it again, as described in *Connect the identity provider*.
3. Enable federation for the domain, as described in *Enable federation for the domain*.

6.10 Where to get help

- The [Univention Help](#) forum for questions from the community.
- Your Univention support contract for a supported environment.

When you report a problem, attach the relevant part of `/var/log/univention/asm.log`.

CHANGELOG

This chapter lists the changes of every released version of the app.

7.1 v6.0.0 (2026-10-19)

- The connector synchronizes to several Apple School Manager accounts. Each account receives only the schools that you assign to it.
- The settings file `/etc/asm-connections.json` replaces the app settings `asm/username`, `asm/password`, and `asm/school_whitelist` and all `asm/attributes/*` and `asm/ldap_filter/*` UCR variables. The settings for students and teachers apply per account, the settings for classes and the LDAP filters per school. The update moves the former values to the new file, as described in [Update from an earlier version](#).
- An error during the upload to one account, for example an invalid LDAP filter, only stops the upload to that account.
- `asm/last_upload/ACCOUNT` holds the time of the last upload to each account.
- The connector no longer checks whether the domain of an email address resolves. The check only wrote a warning, and Apple School Manager accepts such addresses.
- The app supports Keycloak as identity provider for Apple School Manager. Users sign in to their Managed Apple Accounts with the password from the UCS@school domain. See [Keycloak as identity provider for ASM](#).

7.2 v5.1.1 (2026-03-05)

- The connector supports running on a central Replica Directory Node again.

7.3 v5.1.0

- The connector exports more additional locations for students and teachers.

7.4 v5.0.3

- The app refuses installation on a central Replica Directory Node.

7.5 v5.0.2

- Follow-up release for version 5.0.1. A mismatched component ID in the App Center prevented the update from UCS 5.0.

7.6 v5.0.1

- First release for UCS@school 5.2. Functionally identical to version 3.0.3.

7.7 v4.0.0

- First release for UCS@school 5.1. Functionally identical to version 3.0.3.

7.8 v3.0.3

- Fixed a Debian dependency.

7.9 v3.0.2

- The connector exports the grade level, configured with `asm/attributes/student/grade_level`.

7.10 v3.0.1

- The log rotation of the connector follows the `logrotate/*` UCR variables.

7.11 v2.2.4

- The connector applies configured LDAP filters correctly when it loads classes.

7.12 v2.2.3

- Fixed the handling of unexpected errors.

7.13 v2.2.2

- The name of a course, which the connector derives from the school class, follows the pattern in `asm/attributes/course-name-pattern`. The default is `{ou}-{name}`.

7.14 v2.2.1

- The connector applies configured LDAP filters to `rosters.csv`.

7.15 v2.2.0

- The connector uses the name of the school class as the course name. It used the description of the school class before.
- LDAP filters give you finer control over the exported teachers and students. Set them globally or per school with `asm/ldap_filter/students` and `asm/ldap_filter/staff`. An invalid filter stops the synchronization without an export.

7.16 v2.1.0

- The connector fills the `password_policy` column for new students from `asm/attributes/student/password_policy`.

7.17 v2.0.0

- First release for UCS 4.4. Functionally identical to version 1.2.

7.18 v1.2.0

- The connector handles classes with more than 15 teachers correctly. It exports 15 of them, which is the limit of Apple School Manager.

7.19 v1.1.0

- You can install the app on a Replica Directory Node.

7.20 v1.0.0

- First release.

GLOSSARY

App Center

The Univention App Center, the component of *UCS* with which you install and configure apps.

Apple School Manager

The web service with which educational institutions manage their Managed Apple Accounts, devices, and content. Abbreviated as ASM.

Keycloak

The identity and access management software that UCS ships as an app. It provides the single sign-on of the domain.

OIDC

OpenID Connect, the identity layer on top of OAuth 2.0.

PKCE

Proof Key for Code Exchange, an extension of the OAuth 2.0 authorization code flow.

SSF

Shared Signals Framework, the standard of the OpenID Foundation for sharing security events between an identity provider and the applications that rely on it.

UCR

Univention Configuration Registry, the central configuration database of *UCS*.

UCS

Univention Corporate Server, the server operating system with integrated identity management.

UCS@school

The extension of *UCS* for schools and school authorities.

UMC

Univention Management Console, the web interface for the administration of *UCS*.

BIBLIOGRAPHY

BIBLIOGRAPHY

- [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](#)

E

environment variable

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

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

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](#)