univention
be open.

# UCS@school


## Handbuch für Administratoren

www.univention.de

Version 3.1-0
Stand: 14. Februar 2013


Univention GmbH
Mary-Somerville-Straße 1
28359 Bremen
Deutschland
feedback@univention.de

univention
be open.

# Inhaltsverzeichnis

# Kapitel 1. Einführung

UCS@school ist eine auf Univention Corporate Server (UCS) basierende IT-Komplettlösung mit zahlreichen Zusatzkomponenten für Nutzung, Betrieb und Management von Informationstechnologie (IT) in Schulen. UCS@school vereint die Stärken des Enterprise-Betriebssystems UCS im Bereich einfacher und zentraler Verwaltung von IT-Umgebungen mit den Vorteilen klassischer Schulsoftware für den Computereinsatz im Unterricht.

UCS ist die ideale Plattform für Schulen und Schulträger, um IT gemeinsam mit den dazu gehörenden Service- und Supportprozessen für eine oder mehrere Schulen zentral und wirtschaftlich bereitzustellen. UCS@school ergänzt UCS um zahlreiche Komponenten für den IT-Betrieb und den IT-gestützten Unterricht in der Schule.

Die Univention Management Console ermöglicht die zentrale, web-basierte Verwaltung aller Domänendaten (z.B. Benutzer, Gruppen, Rechner, DNS/DHCP). Die Speicherung der Daten erfolgt in einem Verzeichnisdienst auf Basis von OpenLDAP. Da viele Schuldaten primär in schulträgerspezifischen Systemen erfasst werden, bringt UCS@school unter anderem eine CSV-Datei-basierte Importschnittstelle für Schülerdaten mit.

Um den IT-gestützten Unterricht zu ergänzen, wurde die Benutzeroberfläche der Univention Management Console an die Anforderungen von Lehrern angepasst. Dies ermöglicht zum Beispiel die Organisation der Unterrichtsvorbereitung und Klassenraumplanung sowie die temporäre Sperrung des Internetzugangs für ausgewählte Computer. Lehrern ist es auch möglich, den Bildschirminhalt eines Schüler-PCs einzusehen, via Netzwerk individuelle Hilfestellungen zu geben oder einen beliebigen Desktop auf alle anderen Computer in der Klasse oder per Beamer zu übertragen. Auch bei im Schulalltag wiederkehrenden Tätigkeiten, wie dem Zurücksetzen von Passwörtern für Schüler-Benutzerkonten, werden Lehrer unterstützt.

Für die Bedienung der UCS@school-spezifischen Module der Univention Management Console steht ein zusätzliches Dokument [ucs-school-teacher] bereit.

# Kapitel 2. Aufbau einer UCS@school-Umgebung



Univention Corporate Server (UCS) bietet ein plattformübergreifendes Domänenkonzept mit einem gemeinsamen Vertrauenskontext zwischen Linux- und Windows-Systemen. Innerhalb einer UCS-Domäne ist ein Benutzer mit seinem Benutzernamen und Passwort auf allen Systemen bekannt, und kann für ihn freigeschaltete Dienste nutzen.

UCS@school baut auf das flexible Domänenkonzept von UCS auf und integriert einige schulspezifische Erweiterungen.

## 2.1. UCS@school-Benutzerrollen



In einer Standard-UCS-Installation sind alle Benutzerkonten vom selben Typ und unterscheiden sich nur anhand ihrer Gruppenmitgliedschaften. In einer UCS@school-Umgebung ist jeder Benutzer einer *Rolle* zugeordnet, aus der sich Berechtigungen in der UCS@school-Verwaltung ergeben:

- *Schülern* wird in der Standardeinstellung kein Zugriff auf die Administrationsoberflächen gewährt. Sie können sich mit ihren Benutzerkonten nur an Windows-Clients anmelden und die für sie freigegebenen Dateifreigaben und Drucker verwenden.
- *Lehrer* erhalten gegenüber Schülern zusätzliche Rechte, um z.B. auf UMC-Module zuzugreifen, die das Zurücksetzen von Schülerpasswörtern oder das Auswählen von Internetfiltern ermöglichen. Die einem Lehrer angezeigten Module können individuell definiert werden, Lehrer erhalten in der Regel aber nur Zugriff auf einen Teil der von der Univention Management Console bereitgestellten Funktionen.
- Vollen Zugriff auf die Administrationsfunktionen von UCS@school erhalten die *Schuladministratoren*. Sie können z.B. Computer zu Rechnergruppen zusammenfassen, neue Internetfilter definieren oder auch Lehrerpasswörter zurücksetzen.
- Der Benutzertyp *Mitarbeiter* kommt häufig im Umfeld der Schulverwaltung zum Einsatz. Er besitzt in der Standardeinstellung ähnliche Zugriffsrechte wie ein Schülerkonto, kann jedoch mit zusätzlichen Rechten ausgestattet werden.
- Die *System-Administratoren* sind Mitarbeiter mit vollem administrativen Zugriff auf die UCS@school-Systeme, also beispielweise ein IT-Dienstleister, der die Schule beim Betrieb der Server unterstützt.

Überschneidungen der Benutzertypen Lehrer, Mitarbeiter und Schuladministrator sind möglich. So können z.B. Benutzerkonten erstellt werden, die eine Nutzung des Kontos als Lehrer und Mitarbeiter ermöglichen.

Für die Pflege der Benutzerkonten stehen mehrere Möglichkeiten zur Verfügung. Die Bearbeitung von Benutzerkonten kann über die Univention Management Console erfolgen. Darüber hinaus bringt UCS@school flexible Importskripte mit. Sie lesen Tabulator-getrennte Importdateien ein, die üblicherweise aus vorhandenen Schulverwaltungssystemen extrahiert werden können und so einen automatisierten Abgleich ermöglichen.

## 2.2. Aufteilung von UCS@school



Für den Betrieb von UCS@school an einer einzelnen Schule reicht ein Serversystem aus (dieses wird dann in der UCS-Systemrolle Domänencontroller Master installiert).

Für Schulträger oder große Schulen mit mehreren Standorten oder mit einer großen Anzahl an Clients, kann die UCS@school-Installation auf mehrere Server verteilt werden. Dabei wird ein Domänencontroller Master als der primäre Server zur Datenverwaltung genutzt. Für jeden Schul-Standort wird dann ein Domänencontroller Slave installiert, nachfolgend als *Schulserver* bezeichnet.

UCS@school unterstützt derzeit nur einen Schulserver pro Standort. Darüber hinaus können regulär weitere UCS-Systeme installiert und an den Schul-Standorten betrieben werden. Diese zusätzlichen UCS-Systeme können jedoch nicht in Verbindung mit UCS@school-Funktionalitäten (z.B. Klassenshares oder Druckermoderation) eingesetzt werden.

### 2.2.1. Replikation der LDAP-Daten auf die Schul-Standorte



Ein Schulserver bietet alle an einem Standort verwendeten Dienste an. Die Anfragen an den LDAP-Verzeichnisdienst erfolgen dabei gegen einen lokalen LDAP-Server, der automatisch gegen den Domänencontroller Master fortlaufend repliziert und aktualisiert wird. Dies gewährleistet einen reibungslosen Betrieb, auch wenn die Verbindung zwischen Schulserver und dem zentralen Domänencontroller Master einmal ausfallen sollte.

Aus Sicherheitsgründen speichern die Schulservern nur eine Teilreplikation des LDAP-Verzeichnisses. Nur die für den Schulserver relevanten Teile (z.B. Benutzer und Gruppen der jeweiligen Schule) sowie die globalen Strukturen des LDAP-Verzeichnisses werden auf den Schul-Server übertragen.

Zur Unterteilung der im LDAP-Verzeichnisdienst hinterlegten Objekte und Einstellungen wird für jede Schule im LDAP-Verzeichnis eine eigene *Organisationseinheit* (OU) angelegt. Unterhalb dieser OU werden Container für z.B. Benutzerobjekte, Gruppen, DNS- und DHCP-Einstellungen, usw. angelegt. Diese OUs werden direkt unterhalb der LDAP-Basis angelegt. Der Name einer OU sollte sich auf Buchstaben und Ziffern sowie auf den Bindestrich beschränken, da er z.B. die Grundlage für Gruppen- und Rechnernamen bildet. Häufig kommen hier Schulnummern wie *712* oder zusammengesetzte Kürzel wie *28G01* oder *gymmitte* zum Einsatz.

## 2.3. Verwaltungsnetz vs. Edukativnetz



Die Netze für den edukativen Bereich und für die Schulverwaltung müssen aus organisatorischen oder rechtlichen Gründen in der Regel getrennt werden. In UCS@school kann daher zusätzlich zur Unterteilung in Organisationseinheiten (OU) noch eine Unterteilung der OU in Verwaltungsnetz und Edukativnetz erfolgen.

Diese optionale Unterteilung findet auf Ebene der Serversysteme bzw. der Netzwerksegmente statt und sieht vor, dass mindestens ein Schulserver für das edukative Netz und ein Schulserver für das Verwaltungsnetz betrieben wird.

# Kapitel 3. Installation



UCS@school basiert auf Univention Corporate Server (UCS). UCS@school wird dabei als Repository-Komponente eingebunden. Die Installation von UCS ist im UCS-Handbuch dokumentiert. Nachfolgend wird nur auf ggf. auftretende Unterschiede zur Grundinstallation von Univention Corporate Server sowie die Installation von UCS@school selbst eingegangen.

Im folgenden werden zwei Installationsvarianten beschrieben: die Installation als Single-Server-Lösung und die Installation als verteilte Master-Slave-Umgebung mit Schulservern. Single-Server-Umgebungen können auch nachträglich in Master-Slave-Umgebungen umgewandelt werden, indem Schulserver in die Domäne eingebunden werden.

## 3.1. Installation einer Single-Server-Umgebung

Feedback

### 3.1.1. Installation des DC Master

Feedback

Bei der UCS-Installation muss die Systemrolle *Domänencontroller Master* ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul angezeigt, mit welchem die wizardgesteuerte Konfiguration von UCS@school durchgeführt wird:

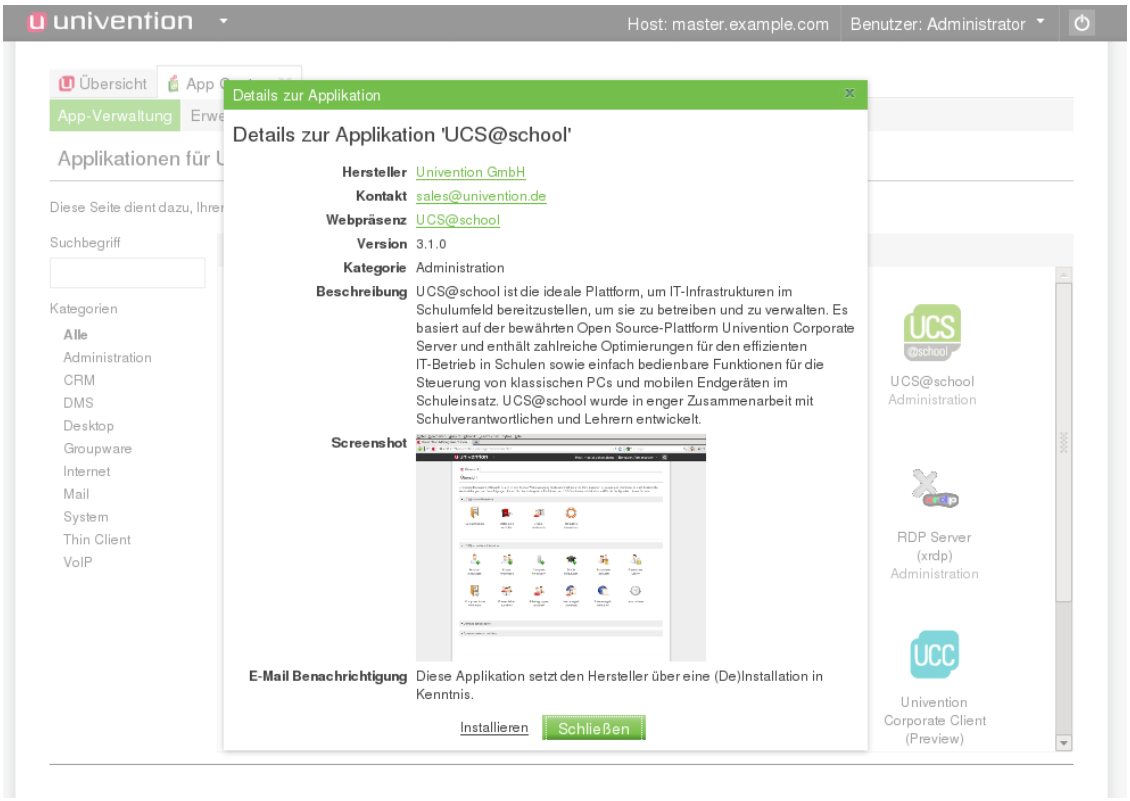
- Das Konfigurationsmodul fragt auf dem DC Master zunächst nach der Art der UCS@school-Umgebung, die installiert werden soll. Hier ist das *Single-Server-Szenario* auszuwählen.

- UCS@school benötigt für die Bereitstellung von Datei- und Drucker-Freigaben den Samba-Dienst. Sofern auf dem DC Master noch kein Samba-Dienst installiert ist, kann zwischen *Samba 3* und *Samba 4* ausgewählt werden.

- Die Daten eines Schulservers werden in Organisationseinheiten (OU) gespeichert. Im letzten Schritt wird nach dem Bezeichner der Schule (OU) gefragt, die vom UMC-Modul im Zuge der Konfiguration automatisch angelegt wird, z.B. *schule719* oder *gymnasium_mitte*.

Während der Konfiguration werden benötigte Softwarepakete automatisch mitinstalliert. Somit sind nach der Konfiguration alle für die Datenpflege und Steuerung von UCS@school benötigten Pakete auf dem DC Master zugreifbar.

**Abbildung 3.1. Installation von UCS@school über das Univention App Center**




Installation und Konfiguration von UCS@school sollten mit einem Neustart des Systems abgeschlossen werden. Im Anschluss kann die weitere Konfguration der Schule vorgenommen werden, siehe Kapitel 5.

## 3.2. Installation einer verteilten Mehr-Server-Umgebung

Feedback

### 3.2.1. Installation des DC Master

Feedback

Bei der UCS-Installation muss die Systemrolle *Domänencontroller Master* ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul *UCS@school-Konfigurationsassistenten* angezeigt, mit welchem die wizardgesteuerte Konfiguration von UCS@school durchgeführt wird:

- Das Konfigurationsmodul fragt auf dem DC Master zunächst nach der Art der UCS@school-Umgebung, die installiert werden soll. Hier ist der Eintrag *verteilte Umgebung* auszuwählen.
- Weitere Konfigurationsoptionen werden in einer verteilten Umgebung auf dem DC Master nicht benötigt.

Während der Konfiguration werden benötigte Softwarepakete automatisch mitinstalliert. Somit sind nach der Konfiguration alle für die Datenpflege benötigten Pakete auf dem DC Master zugreifbar.

Installation und Konfiguration von UCS@school sollten mit einem Neustart des Systems abgeschlossen werden.

### 3.2.2. Installation eines DC Backup (optional)

Feedback

Auf Servern mit der Rolle *Domänencontroller Backup* (kurz DC Backup) werden alle Domänendaten und SSL-Sicherheitszertifikate als Nur-Lese-Kopie gespeichert.

Ein DC Backup dient als Fallback-System des DC Master. Sollte dieser ausfallen, kann ein DC Backup die Rolle des DC Master dauerhaft übernehmen. Der Einsatz eines DC Backup ist optional.

### Anmerkung

Sofern DC Backup-Systeme in der Domäne vorhanden sind, muss dort ebenfalls UCS@school installiert und konfiguriert werden, um durch mitinstallierte LDAP-ACLs eine einheitliche LDAP-Replikation zu gewährleisten. Auf den DC Backup-Systemen muss die Konfiguration über den UCS@school-Konfigurationsassistenten erfolgen, bevor der erste Schulserver installiert und in die Domäne aufgenommen wird.

Die Installation und Konfiguration von UCS@school auf einem DC Backup erfolgt analog zur in Abschnitt 3.2.1 beschriebenen Installation des DC Master.

## 3.2.3. Installation eines Schulserver



An jedem Schul-Standort muss ein Schulserver installiert werden.

Bei der UCS-Installation muss die Systemrolle *Domänencontroller Slave* (kurz DC Slave) ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul angezeigt, mit welchem die wizardgesteuerte Konfiguration von UCS@school auf dem DC Slave durchgeführt wird:

- Das Konfigurationsmodul kann auf einem DC Slave nur dann erfolgreich durchlaufen werden, wenn die Konfiguration des DC Masters bereits über das dort installierte Konfigurationsmodul abgeschlossen wurde.

- Nach der Konfiguration ist es erforderlich, dass der DC Slave erneut der Domäne beitritt. Im zweiten Schritt werden die für den erneuten Beitritt notwendigen Anmeldedaten (Benutzername, Passwort) abgefragt. Hier kann der Benutzer *Administrator* oder ein Mitglieder der Gruppe *Domain Admins* angegeben werden. Der vollqualifizierte Rechnername (FQDN) des DC Masters wird üblicherweise automatisch ermittelt und vorausgefüllt. Sollte dies nicht möglich sein, muss der vollständige Rechnername inkl. DNS-Domäne angegeben werden, z.B. master.example.com.

- UCS@school benötigt für die Bereitstellung von Datei- und Drucker-Freigaben den Samba-Dienst. Sofern auf dem DC Master noch kein Samba-Dienst installiert ist, kann zwischen *Samba 3* und *Samba 4* ausgewählt werden.

- Die Daten eines Schulservers werden in Organisationseinheiten (OU) gespeichert. Im letzten Schritt wird nach dem Bezeichner der Schule (OU) gefragt, die im Zuge der Konfiguration automatisch für diesen Schulserver angelegt werden soll, z.B. *schule719* oder *gymnasium_mitte*.

Während der Konfiguration werden benötigte Softwarepakete automatisch mitinstalliert und ein erneuter Domänenbeitritt durchgeführt. Somit sind nach der Konfiguration alle für die Steuerung von UCS@school benötigten Pakete auf dem DC Slave zugreifbar.

### Anmerkung

Wurde während der Installation des DC Slaves ein DHCP-Server installiert, ist es für die korrekte Funktion des DHCP-Servers notwendig, dass das DHCP-Server-Objekt des DC Slaves (zu finden unter `cn=dhcp,`*`LDAPBASIS`*) in den entsprechenden DHCP-Container der OU verschoben wird (`cn=dhcp,ou=`*`OUNAME`*`,`*`LDAPBASIS`*).

Installation und Konfiguration von UCS@school sollten mit einem Neustart des Systems abgeschlossen werden.

## 3.3. Domänenbeitritt eines Schulservers

Feedback

Die Einrichtung eines Schulservers ist auch ohne das oben beschriebene UMC-Konfigurationsmodul möglich, bzw. notwendig, wenn während des Konfigrationsprozesses Probleme auftreten sollten. Dazu müssen die in diesem Abschnitt beschriebenen Schritte manuell durchgeführt werden.

Vor dem Domänenbeitritt des Schulservers muss die Organisationseinheit des Schulservers in der Univention Management Console des DC Masters angelegt werden (siehe Abschnitt 5.1).

Anschließend muss das System erneut der Domäne beitreten. Dies erfolgt auf der Kommandozeile durch Aufruf des Befehls `univention-join`.

Der Domänencontroller Master wird im Regelfall durch eine DNS-Abfrage ermittelt. Wenn das nicht möglich sein sollte, kann der Rechnername des DC Master auch durch den Parameter `-dcname` *`HOSTNAME`* direkt angegeben werden. Der Rechnername muss dabei als vollqualifizierter Name angegeben werden, also beispielsweise *master.schule.de*.

Als Join-Account wird ein Benutzerkonto bezeichnet, das berechtigt ist, Systeme der UCS-Domäne hinzuzufügen. Standardmäßig ist dies der Benutzer *Administrator* oder ein Mitglied der Gruppe *Domain Admins*. Der Join-Account kann durch den Parameter `-dcaccount` *`ACCOUNTNAME`* an `univention-join` übergeben werden.

# Kapitel 4. Übersicht über die schulspezifischen Anwendungen



## 4.1. Modulübersicht



UCS@school stellt eine Reihe von Modulen für die Univention Management Console bereit, die für den IT-gestützten Unterricht verwendet werden können.

Im folgenden werden die Module kurz beschrieben. Eine ausführliche Beschreibung der Verwendung der Module findet sich im separaten Handbuch für Lehrer [ucs-school-teacher].

Einige Module stehen Lehrern und Schuladministratoren zur Verfügung während andere Module nur Schuladministratoren vorbehalten sind:

- *Passwörter (Schüler)* erlaubt Lehrern das Zurücksetzen von Schüler-Passwörtern. Die bestehenden Schüler-Passwörter können aus Sicherheitsgründen nicht ausgelesen werden; wenn Schüler ihr Passwort vergessen, muss ein neues Passwort vergeben werden. Schuladministratoren dürfen außerdem die Passwörter von Lehrern zurücksetzen.

- Das Modul *Computerraum* erlaubt die Kontrolle der Schüler-PCs und des Internetzugangs während einer Schulstunde. Der Internetzugang kann gesperrt oder freigegeben werden und einzelne Internetseiten können gezielt freigegeben werden. Wenn eine entsprechende Software (iTALC) auf den Schüler-PCs installiert ist, besteht auch die Möglichkeit diese PCs zu steuern. So kann beispielsweise der Bildschirm gesperrt werden, so dass in einer Chemie-Stunde die ungeteilte Aufmerksamkeit auf ein Experiment gelenkt werden kann.

  Außerdem kann der Bildschiminhalt eines PCs auf andere Systeme übertragen werden. Dies erlaubt es Lehrern, auch ohne einen Beamer Präsentationen durchzuführen.

- Jede Schule wird durch einen Helpdesk betreut. Der Helpdesk kann z.B. durch eine Support-Organisation beim Schulträger oder durch technisch versierte Lehrer an den Schulen umgesetzt werden. Über das Modul *Helpdesk kontaktieren* können Lehrer und Schuladministratoren eine E-Mail-Anfrage stellen. Die Konfiguration des Helpdesk-Moduls wird in Abschnitt 5.7 beschrieben.

- Jeder Schüler ist Mitglied seiner Klasse. Darüber hinaus gibt es die Möglichkeit mit dem Modul *Arbeitsgruppen verwalten* Schüler in klassenübergreifende Arbeitsgruppen einzuordnen.

  Das Anlegen einer Arbeitsgruppe legt automatisch einen Datenbereich auf dem Schulserver an, auf den alle Mitglieder der Arbeitsgruppe Zugriff haben.

  Lehrer können Schüler zu Arbeitsgruppen hinzufügen oder entfernen, aber keine neuen Arbeitsgruppen anlegen. Dies muss von einem Schuladministrator vorgenommen werden.

- Das Modul *Arbeitsgruppen verwalten* erlaubt Schuladministratoren neue Arbeitsgruppen anzulegen und diesen neben Schülern auch Lehrer zuzuweisen.

- Mit dem Modul *Drucker moderieren* können Ausdrucke der Schüler geprüft werden. Die anstehenden Druckaufträge können vom Lehrer betrachtet und entweder verworfen oder zum Drucken freigegeben werden. Dadurch können unnötige oder fehlerhafte Ausdrucke vermieden werden.

- Das Modul *Materialien verteilen* vereinfacht das Verteilen und Einsammeln von Unterrichtsmaterial an Klassen oder Arbeitsgruppen. Optional kann eine Frist zum Verteilen und Einsammeln festgelegt werden.

So ist es möglich, Aufgaben zu verteilen, die bis zum Ende der Unterrichtsstunde zu bearbeiten sind. Nach Ablauf der Frist werden die verteilten Materialien dann automatisch wieder eingesammelt und im Heimatverzeichnis des Lehrers abgelegt.

- Mit dem Modul *Computerräume verwalten* werden Computer einer Schule einem Computerraum zugeordnet. Diese Computerräume können von den Lehrern zentral verwaltet werden, etwa indem der Internetzugang freigegeben wird.
- Das Modul *Unterrichtszeiten* erlaubt es, die Zeiträume der jeweiligen Schulstunden pro Schule zu definieren.
- Für jede Klasse gibt es einen gemeinsamen Datenbereich. Damit Lehrer auf diesen Datenbereich zugreifen können, müssen sie mit dem Modul *Lehrer Klassen zuordnen* der Klasse zugewiesen werden.
- Für die Filterung des Internetzugriffs wird ein Proxy-Server eingesetzt, der bei dem Abruf einer Internetseite prüft, ob der Zugriff auf diese Seite erlaubt ist. Ist das nicht der Fall, wird eine Informationsseite angezeigt. Dies wird in Kapitel 8 weitergehend beschrieben.

  Wenn Schüler beispielsweise in einer Schulstunde in der Wikipedia recherchieren sollen, kann eine Regelliste definiert werden, die Zugriffe auf alle anderen Internetseiten unterbindet. Diese Regelliste kann dann vom Lehrer zugewiesen werden.

  Mit der Funktion **Internetregeln definieren** können die Regeln verwaltet werden.

# Kapitel 5. Einrichtung einer Schule



## 5.1. Registrierung einer Schule

Feedback

Die Daten eines Schulservers werden in einer Organisationseinheit (OU) - einem Teilbaum des LDAP-Verzeichnisses - gespeichert. Nur die für einen Schulserver relevanten Daten werden dorthin übertragen.

Eine Schule, die mit UCS@school verwaltet werden soll, muss in der Univention Management Console auf dem Domänencontroller Master registriert werden. Dort muss in der Modulgruppe *UCS@school Administration* das Modul **Schule hinzufügen** aufgerufen werden.

Als **Name der Schule** ist ein Bezeichner für die Schule einzutragen, z.B. *schule719* oder *gymnasium-mitte*. Der **Rechnername des Schulservers** ist der Name des Schulservers. In einer Single-Server-Umgebung ist die Angabe nicht erforderlich. Nach dem erfolgreichen Anlegen der Schule erscheint eine Statusmeldung.

Wurde ein Schulserver angegeben, wird dieser automatisch als Dateiserver für Klassen- und Benutzerfreigaben verwendet (siehe Abschnitt 7.2).

Wenn der Schulserver für diese Schule schon installiert wurde, sollte das System nun der Domäne beitreten (siehe Abschnitt 3.3), bevor Schülerkonten angelegt werden können.

## 5.2. Import der Benutzerkonten

Feedback

Der Import der Schüler-, Lehrer- und Mitarbeiterdaten erfolgt in der Regel zentral für den gesamten Schulträger und ist in Kapitel 6 beschrieben.

## 5.3. Import der Rechnerkonten für die Windows-PCs

Feedback

Rechner können entweder manuell oder über ein Import-Skript angelegt werden.

Die Daten eines Schulservers werden in einer Organisationseinheit (OU) - einem Teilbaum des LDAP-Verzeichnisses - gespeichert. Nur die für einen Schulserver relevanten Daten werden dorthin übertragen.

Anschließend treten die Windows-PCs, wie im UCS-Handbuch beschrieben, der Domäne bei.

## 5.4. Anlegen eines einzelnen PCs

Feedback

Ein einzelner Schul-PC kann in der Univention Management Console auf dem Domänencontroller Master registriert werden. Dort muss in der Modulgruppe *UCS@school Administration* das Modul **Computer hinzufügen** aufgerufen werden. Existiert mehr als eine Schule, ist die entsprechende Schule auszuwählen. Es

stehen zwei Arten von Rechnern zur Auswahl: **Windows-Systeme** oder ein **Gerät mit IP-Adresse** (z.B. ein Netzwerkdrucker mit eigener IP-Adresse).

Die Angabe von **Name**, **IP-Adresse** und **MAC-Adresse** ist verpflichtend. Die **Subnetzmaske** kann in den meisten Fällen auf der Voreinstellung belassen werden. Die MAC-Adresse ist nötig für die Vergabe der IP-Adressen per DHCP.

## 5.5. Skriptbasierter Import von PCs



Der Import mehrerer PCs erfolgt über das Skript `/usr/share/ucs-school-import/scripts/import_computer`, das auf dem Domänencontroller Master als Benutzer *root* aufgerufen werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter, die in folgender Syntax definiert wird. Die einzelnen Felder sind durch ein Tabulatorzeichen zu trennen.

Es ist zu beachten, dass Computernamen domänenweit eindeutig sein müssen. Das heißt ein Computer *windows01* kann nicht in mehreren OUs verwendet werden. Um die Eindeutigkeit zu gewährleisten, wird empfohlen, jedem Computernamen die OU voranzustellen oder zu integrieren (z.B. *712win01* für Schule *712*).

| Feld | Beschreibung | Mögliche Werte | Beispiel |
|---|---|---|---|
| Rechnertyp | Typ des Rechnerobjektes | ipmanagedclient, macos, windows | windows |
| Name | Zu verwendender Rechnername | --- | win28g01-01 |
| MAC-Adresse | MAC-Adresse (wird für DHCP benötigt) | --- | 00:0c:29:12:23:34 |
| OU | OU, in der das Rechnerobjekt modifiziert werden soll | --- | 28G01 |
| IP-Adresse (/ Netzmaske) | IP-Adresse des Rechnerobjektes und optional die passende Netzmaske | --- | 10.0.5.45/255.255.255.0 |
| (Inventarnr.) | Optionale Inventarnummer | --- | TR47110815-XA-3 |
| (Zone) | Optionale Zone | edukativ, verwaltung | edukativ |

Die Subnetzmaske kann sowohl als Prefix (*24*) als auch in Oktettschreibweise (*255.255.255.0*) angegeben werden. Die Angabe der Subnetzmaske ist optional. Wird sie weggelassen, wird die Subnetzmaske 255.255.255.0 angenommen.

Wird im Feld *IP-Adresse (/ Netzmaske)* nur ein Subnetz angegeben (z.B. 10.0.5.0), wird dem Computerobjekt automatisch die nächste freie IP-Adresse aus diesem Subnetz zugewiesen.

Beispiel für eine Importdatei:

```
ipmanagedclient  router28g01-01   10:00:ee:ff:cc:02  28G01 10.0.5.1
windows    win28g01-01   10:00:ee:ff:cc:00  28G01 10.0.5.5
windows    win28g01-02   10:00:ee:ff:cc:01  28G01 10.0.5.6
macos    mac28g01-01   10:00:ee:ff:cc:03  28G01 10.0.5.7
ipmanagedclient  printer28g01-01  10:00:ee:ff:cc:04  28G01 10.0.5.250
```

Die importierten Rechner werden so konfiguriert, dass ihnen die angegebene IP-Adresse automatisch per DHCP zugeordnet wird (sofern auf dem Schulserver der DHCP-Dienst installiert ist) und der angegebene Rechnername über das Domain Name System (DNS) aufgelöst werden kann.

## 5.6. Konfiguration von Druckern an der Schule

Feedback

Der Import der Drucker kann skriptbasiert über das Skript `/usr/share/ucs-school-import/scripts/import_printer` erfolgen, das auf dem Domänencontroller Master als Benutzer *root* aufgerufen werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter, die in folgender Syntax definiert wird. Die einzelnen Felder sind durch ein Tabulatorzeichen zu trennen.

| **Feld** | **Beschreibung** | **Mögliche Werte** | **Beispiel** |
|---|---|---|---|
| Aktion | Art der Druckermodifkation | *A*=Hinzufügen, *M*=Modifizieren, *D*=Löschen | A |
| OU | OU, in der das Druckerobjekt modifiziert werden soll | --- | 28G01 |
| Druckserver | Name des zu verwendenden Druckservers | --- | dc28g01-01 |
| Name | Name der Druckerwarteschlange | --- | laserdrucker |
| URI | URI, unter dem der Drucker erreichbar ist | --- | lpd://10.0.5.250 |

Die Druckerwarteschlange wird beim Anlegen eines neuen Druckers auf dem im Feld *Druckserver* angegebenen Druckserver eingerichtet. Das URI-Format unterscheidet sich je nach angebundenem Drucker und ist im Druckdienste-Kapitel des UCS-Handbuchs beschrieben.

## 5.7. Konfiguration der Helpdesk-Kontaktadresse

Feedback

Über das Helpdesk-Modul können Lehrer per E-Mail Kontakt zum Helpdesk-Team einer Schule aufnehmen. Damit dieses Modul genutzt werden kann, muss auf dem jeweiligen Server die Univention Configuration Registry-Variable `ucsschool/helpdesk/recipient` auf die E-Mail-Adresse des zuständigen Helpdesk-Teams gesetzt werden.

## 5.8. Skriptbasierter Import von Netzwerken

Feedback

Netzwerke können über das Skript `/usr/share/ucs-school-import/scripts/import_networks` importiert werden. Das Skript muss auf dem Domänencontroller Master als Benutzer *root* aufgerufen werden. Das Format der Import-Datei ist wie folgt aufgebaut:

| **Feld** | **Beschreibung** | **Mögliche Werte** |
|---|---|---|
| OU | OU des zu modifizierenden Netzwerks | 28G01 |
| Netzwerk | Netzwerk und Subnetzmaske | 10.0.5.0/255.255.255.0 |
| (IP-Adress-Bereich) | Bereich, aus dem IP-Adressen für neuangelegte Systeme automatisch vergeben werden | 10.0.5.10-10.0.5.140 |
| (Router) | IP-Adresse des Routers | 10.0.5.1 |
| (DNS-Server) | IP-Adresse des DNS-Servers | 10.0.5.2 |
| (WINS-Server) | IP-Adresse des WINS-Servers | 10.0.5.2 |

Beispiel für eine Importdatei:

```
28G01  10.0.5.0                              10.0.5.1  10.0.5.2  10.0.5.2
28G01  10.0.6.0/25  10.0.6.5-10.0.6.120       10.0.6.1  10.0.6.2  10.0.6.15
```

Wird für das Feld *Netzwerk* keine Netzmaske angegeben, so wird automatisch die Netzmaske *255.255.255.0* verwendet. Sollte der *IP-Adressbereich* nicht explizit angegeben worden sein, wird der Bereich *X.Y.Z.20-X.Y.Z.250* verwendet.

Zur Vereinfachung der Administration der Netzwerke steht zusätzlich das Skript `import_router` zur Verfügung, das nur den Default-Router für das angegebene Netzwerk neu setzt. Es verwendet das gleiche Format wie `import_networks`.

## 5.9. Anlegen von Freigaben

Feedback

Die meisten Freigaben in einer UCS@school-Umgebung werden automatisch erstellt; jede Klasse oder Arbeitsgemeinschaft verfügt über eine gemeinsame Freigabe. Weiterhin existiert mit der *Marktplatz*-Freigabe je Schule eine schulweite Freigabe. Das Erstellen der Marktplatzfreigabe beim Anlegen einer OU kann durch das Setzen der Univention Configuration Registry-Variable `ucsschool/import/generate/markt-platz` auf den Wert *no* verhindert werden.

Diese Freigaben müssen zwingend auf dem Schulserver bereitgestellt werden, um die von UCS@school bereitgestellten Funktionen nutzen zu können.

Weitere Freigaben werden, wie in einer Standard-UCS-Installation, über das UMC-Modul **Freigaben** auf dem Domänencontroller Master angelegt. Weiterführende Dokumentation findet sich im Freigaben-Kapitel des UCS-Handbuchs [ucs-handbuch].

Die Freigaben müssen unterhalb der OU der Schule angelegt werden, die Auswahl findet mit der Option **Container** beim Anlegen einer Freigabe statt. Bei eine OU *gym17* muss beispielsweise *gym17/shares* ausgewählt werden.

## 5.10. Anlegen von Schuladministratoren

Feedback

Benutzerkonten für Schuladministratoren können über das UMC-Modul **Benutzer** auf dem Domänencontroller Master angelegt werden.

Die Schuladministratoren müssen unterhalb der OU der Schule im Container *cn=users,cn=admins* angelegt werden. Die Auswahl findet mit der Option **Container** beim Anlegen eines Benutzers statt. Bei einer OU *gym17* muss beispielsweise *gym17/users/admins* ausgewählt werden.

Der Benutzer muss außerdem im Reiter **Gruppen** in die Gruppe *admins-OU*, also z.B. *admins-gym17*.

Wenn der Schuladministrator auch als Lehrer tätig ist, muss der Benutzer außerdem in die Gruppe *lehrer-OU* aufgenommen, also z.B. *lehrer-gym17*.

## 5.11. Anlegen eines PDF-Druckers für die Druckermoderation

Feedback

Druckerfreigaben werden, wie in einer Standard-UCS-Installation, über das UMC-Modul **Drucker** auf dem Domänencontroller Master angelegt. Weiterführende Dokumentation findet sich im Druckdienste-Kapitel des UCS-Handbuchs [ucs-handbuch].

Die Drucker müssen unterhalb der OU der Schule angelegt werden, die Auswahl findet mit der Option **Container** beim Anlegen eines Drucker statt. Bei der OU *gym17* muss beispielsweise *gym17/printers* ausgewählt werden.

Für die Verwendung der Druckermoderation muss ein PDF-Drucker eingerichtet werden. Dieser muss ebenfalls unterhalb der Schul-OU angelegt werden. Dabei müssen folgende Werte gesetzt werden:

- **Server** : Name des Schulservers
- **Protokoll** : *cups-pdf:/*
- **Ziel** : leer
- **Drucker-Hersteller** : *PDF*
- **Drucker-Modell** : *Generic CUPS-PDF Printer*

## 5.12. Anlegen von Mitarbeitern



Mitarbeiter werden über das UMC-Modul **Benutzer** auf dem Domänencontroller Master angelegt.

Die Mitarbeiterkonten müssen unterhalb der OU der Schule im Container *cn=users,cn=mitarbeiter* angelegt werden, die Auswahl findet mit der Option **Container** beim Anlegen eines Benutzers statt. Bei einer OU *gym17* muss beispielsweise *gym17/users/mitarbeiter* ausgewählt werden.

Der Benutzer muss außerdem im Reiter **Gruppen** in die Gruppe *mitarbeiter-OU*, also z.B. *mitarbeiter-gym17*.

# Kapitel 6. Verwaltung von Schüler- und Lehrerdaten



## 6.1. Import der Schüler- und Lehrerdaten



Die Verwaltung der Schüler- und Lehrerdaten und deren Aktualisierung zum Schuljahreswechsel (Versetzungen, Schulabgänge etc.) erfolgt in der Regel durch die Schulverwaltung. Hierbei wird eine große Anzahl an Lösungen zur Datenpflege eingesetzt, die sich von Schulträger zu Schulträger unterscheidet.

Die Benutzerverwaltung von UCS@school ist darauf ausgelegt, dass die primäre Verwaltung der Schuldaten weiterhin durch die Schulverwaltung erfolgt. Diese Daten werden dann in eine Datei im CSV-Format exportiert und in UCS@school importiert. Die einzelnen Felder der CSV-Datei sind durch ein Tabulatorzeichen zu trennen.

Für punktuelle Anpassungen - etwa ein Schulwechsel mitten im Schuljahr - besteht auch die Möglichkeit einzelne Schüler manuell anzulegen. Dies wird im UCS@school-Handbuch für Lehrkräfte beschrieben.

Der Import der Schuldaten ist bei Single-Server- und verteilten Umgebungen identisch.

Der Import von Benutzern erfolgt über das Skript `/usr/share/ucs-school-import/scripts/import_user`, das auf dem Domänencontroller Master als Benutzer *root* gestartet werden muss. Es erwartet den Namen einer CSV-Datei als ersten Parameter. Das Format der Eingabedatei ist wie folgt aufgebaut:

**Tabelle 6.1. Aufbau der Datenzeilen für den Benutzer-Import**

| Feld | Beschreibung | Mögliche Werte | Beispiel |
|---|---|---|---|
| Aktion | Art der Benutzermodifikation | *A*=Hinzufügen, *M*=Modifizieren, *D*=Löschen | A |
| Benutzername | Der zum Login verwendete Benutzername | --- | m.mustermann |
| Nachname | Der Nachname des Benutzers | --- | Mustermann |
| Vorname | Der Vorname des Benutzers | --- | Michael |
| OU | Die OU, unter der der Benutzer angelegt werden soll | --- | 28G01 |
| Klasse | Name der Klasse des Benutzers; nur Lehrer können in mehreren Klassen vertreten sein! | --- | 1A,1B,2A,4C |
| Rechte | derzeit ungenutzt; das Feld sollte leer bleiben, so dass 2 Tabulator-Zeichen aufeinander folgen | --- | |
| Email-Adresse | Mailadresse des Benutzers | --- | m.musterm@beispiel.edu |
| (Lehrer) | Definiert, ob der Benutzer ein Lehrer ist | *0*=Kein Lehrer, *1*=Lehrer | 1 |

| Feld | Beschreibung | Mögliche Werte | Beispiel |
|---|---|---|---|
| (Aktiv) | Definiert, ob das Benutzerkonto beim Anlegen sofort aktiviert wird | *0*=nicht aktivieren, *1*=aktivieren | 1 |
| (Mitarbeiter) | Definiert, ob der Benutzer ein Mitarbeiter ist | *0*=Kein Mitarbeiter, *1*=Mitarbeiter | 0 |

Ein Beispiel für eine Importdatei:

```
A  max          Mustermann  Max     28G01  1A         max@schule.edu   0 1
 0
M  m.musterma   Mustermann  Moritz  28G01  1A,2D,4C   m.m@schule.edu   1 1
 0
D  a.musterfr   Musterfrau  Anke    28G01  2B         a.mfr@schule.edu 1 1
 1
```

Über das Feld *Aktion* kann die Art der Benutzermodifikation gesteuert werden. Folgende Aktionen sind definiert:

| Aktion | Beschreibung |
|---|---|
| A | Hinzufügen |
| M | Modifizieren |
| D | Löschen |

Auch beim Löschen (Aktion *D*) müssen gültige Werte übergeben werden.

Die Angabe von Klassen bezieht sich bei Schülern in der Regel auf eine einzelne Klasse. Lehrer können dagegen in mehreren Klassen vertreten sein. Diese sollten auch angegeben werden (kommasepariert), damit die Benutzerkonten der Lehrer automatisch in die jeweilige Klassengruppe eingetragen werden und sie somit auch Zugriff auf die jeweilige Dateifreigabe der Klasse erhalten.

Die optionalen Felder *Lehrer* und *Mitarbeiter* bestimmen die Rolle des Benutzers im System. Werden die Werte nicht angegeben, so wird der Benutzer mit der Rolle Schüler angelegt. Es ist möglich einem Benutzer sowohl die Rollen Lehrer und Mitarbeiter zu geben.

Über das optionale Feld *Aktiv* wird gesteuert, ob das Benutzerkonto aktiviert werden soll. Ist kein Wert angegeben, wird das Konto automatisch aktiviert.

Die Benutzerkonten werden mit einem zufälligen, unbekannten Passwort initialisiert. Mehrere Personengruppen können die Konten freischalten:

- Das Konto eines Schuladministrators kann durch einen administrativen Mitarbeiter in der Univention Management Console festgelegt werden.
- Die Konten von Lehrern können durch den Schuladministrator über das Modul **Passwörter (Schüler)** durch Vergabe eines Passworts freigeschaltet werden.
- Die Konten von Schülern können durch Lehrer über das Modul **Passwörter (Lehrer)** klassenweise durch Vergabe eines Passworts freigeschaltet werden.

Mit den folgenden Univention Configuration Registry-Variablen kann für Schüler, Lehrer, Schuladministratoren und Mitarbeiter eine UMC-Richtlinie zugewiesen werden, die festlegt, welche UMC-Module bei einer Anmeldung der entsprechenden Benutzergruppe angezeigt werden. Hierbei muss der LDAP-DN (Distinguished Name) der Richtlinie angegeben werden.

- `ucsschool/ldap/default/policy/umc/pupils` gilt für Anmeldungen von Schülern

- `ucsschool/ldap/default/policy/umc/teachers` gilt für Anmeldungen von Lehrern
- `ucsschool/ldap/default/policy/umc/admins` gilt für Anmeldungen von Schuladministratoren
- `ucsschool/ldap/default/policy/umc/staff` gilt für Anmeldungen von Mitarbeitern

Wenn die UCR-Variablen auf den Wert *None* gesetzt sind, wird für den jeweiligen Benutzertyp keine Richtlinie verknüpft. Es müssen dann eigene Richtlinien an die Container gebunden werden.

## 6.2. Skriptgesteuerter Import von Klassen oder Arbeitsgruppen



Klassen und Arbeitsgruppen werden in der Regel durch die entsprechenden UMC-Module verwaltet (siehe UCS@school-Lehrerhandbuch [ucs-school-teacher]). Es besteht jedoch auch die Möglichkeit, Klassen skriptbasiert zu importieren.

Es ist zu beachten, dass die Klassennamen domänenweit eindeutig sein müssen. Das heißt eine Klasse *1A* kann nicht in mehreren OUs verwendet werden. Daher sollte jedem Klassennamen die OU vorangestellt werden. Bei der Erstellung von Klassen über das UMC-Modul *Klasse hinzufügen* geschieht dies automatisch. Sprechende Namen, wie zum Beispiel *Igel* oder *BiologieAG*, sind für Klassennamen ebenso möglich wie Buchstaben-Ziffern-Kombinationen (*10R*). Beispiele für die Schule gym123:

```
gym123-1A
gym123-1B
gym123-2A
gym123-Igel
```

Das Dateiformat für die Gruppen-Importdatei ist wie folgt aufgebaut:

**Tabelle 6.2. Aufbau der Datenzeilen für den Gruppen-Import**

| Feld | Beschreibung | Mögliche Werte | Beispiel |
|---|---|---|---|
| Aktion | Art der Gruppenmodifikation | *A*=Hinzufügen, *M*=Modifizieren, *D*=Löschen | A |
| OU | OU, in der die Gruppe modifiziert werden soll | --- | 28G01 |
| Gruppenname | Der Name der Gruppe | --- | 28G01-1A |
| (Beschreibung) | Optionale Beschreibung der Gruppe | --- | Klasse 1A |

Ein Beispiel für eine Importdatei:

```
A     28G01     28G01-1A         Klaaassen 1A
A     28G01     28G01-LK-Inf     Leistungskurs Informatik
M     28G01     28G01-1A         Klasse 1A
D     28G01     28G01-LK-Inf     Leistungskurs Informatik
D     28G01     28G01-R12        Klasse R12
```

## 6.3. Vorgehen zum Schuljahreswechsel



Zum Schuljahreswechsel stehen zahlreiche Änderungen in den Benutzerdaten an: Schüler werden in eine höhere Klasse versetzt, der Abschlussjahrgang verlässt die Schule und ein neuer Jahrgang wird eingeschult.

Ein Schuljahreswechsel erfolgt in vier Schritten:

1. Eine Liste aller Schulabgänger wird aus der Schulverwaltungssoftware exportiert und die Konten werden über das Import-Skript entfernt (Aktion D, siehe Abschnitt 6.1). Die Klassen der Schulabgänger müssen ebenfalls über das Import-Skript für Gruppen entfernt werden.

2. Die bestehenden Klassen sollten umbenannt werden. Dies stellt sicher, dass Dateien, die auf einer Klassenfreigabe gespeichert werden und somit einer Klasse zugeordnet sind, nach dem Schuljahreswechsel weiterhin der Klasse unter dem neuen Klassennamen zugeordnet sind.

   Die ältesten Klassen (die der Abgänger zum Schulende) müssen zuvor gelöscht werden. Die Umbenennung erfolgt über das Skript `/usr/share/ucs-school-import/scripts/rename_class`, das auf dem Domänencontroller Master als Benutzer *root* aufgerufen werden muss. Es erwartet den Namen einer tab-separierten CSV-Datei als ersten Parameter. Die CSV-Datei enthält dabei pro Zeile zuerst den alten und dann den neuen Klassennamen, z.B.

   ```
   gymmitte-6B  gymmitte-7B
   gymmitte-5B  gymmitte-6B
   ```

   Die Reihenfolge der Unbenennung ist wichtig, da die Umbenennung sequentiell erfolgt und der Zielname nicht existieren darf.

3. Eine aktuelle Liste aller verbleibenden Schülerdaten wird über das Import-Skript neu eingelesen (Aktion M, siehe Abschnitt 6.1).

4. Eine Liste aller Neuzugänge wird aus der Schulverwaltungssoftware exportiert und über das Import-Skript importiert (Aktion A, siehe Abschnitt 6.1).

# Kapitel 7. Integration und Verwaltung von Microsoft Windows-Clients



Microsoft Windows-Clients werden in Univention Corporate Server (UCS) mithilfe von Samba integriert und verwaltet. Die Windows-Clients authentifizieren sich dabei gegen den Samba-Server. Auch Datei- und Druckdienste werden für die Windows-Clients über Samba bereitgestellt. Weitere Hinweise finden sich in Abschnitt 7.1.

Die Netzkonfiguration der Clients kann zentral über in UCS integrierte DNS- und DHCP-Dienste durchgeführt werden. Weitere Hinweise finden sich in Abschnitt 5.5.

Auf den Windows-Clients der Schüler kann die Software *iTALC* installiert werden. Sie erlaubt es Lehrern, über ein UMC-Modul den Desktop der Schüler einzuschränken und z.B. Bildschirme und Eingabegeräte zu sperren. Außerdem kann ein Übertragungsmodus aktiviert werden, der die Bildschirmausgabe des Desktops des Lehrers auf die Schülerbildschirme überträgt. Die Installation von iTALC wird in Abschnitt 7.3 beschrieben.

## 7.1. Anmeldedienste mit Samba



In Univention Corporate Server 3.x stehen zwei verschiedene Samba-Varianten zur Auswahl:

- *Samba 3* implementiert Domänendienste auf Basis der Domänen-Technologie von Microsoft Windows NT. Samba 3 ist die aktuelle stabile und bewährte Haupt-Release-Serie des Samba-Projekts und ist seit vielen Jahren in UCS integriert.

- *Samba 4* ist die nächste Generation der Samba-Suite. Die wichtigste Neuerung von Samba 4 besteht in der Unterstützung von Domänen-, Verzeichnis- und Authentifizierungsdiensten, die kompatibel zu Microsoft Active Directory sind. Mit Samba 4 lassen sich deswegen Active Directory-kompatible Windows-Domänen aufbauen. Diese ermöglichen auch die Verwendung der von Microsoft bereit gestellten Werkzeuge beispielsweise für die Verwaltung von Benutzern oder Gruppenrichtlinien (GPOs). Die aktuell vom Samba-Projekt veröffentlichten Versionen von Samba 4 unterliegen in der Weiterentwicklung noch stärkeren Änderungen als Samba 3. Univention hat die benötigten Komponenten für die Bereitstellung von Active Directory kompatiblen Domänendiensten mit Samba 4 getestet und in enger Zusammenarbeit mit dem Samba-Team in UCS integriert. Parallel dazu wurde für UCS Samba 3 mit Samba 4 integriert. Somit werden auch bei Verwendung der Active Directory kompatiblen Domänendienste die erprobten Datei- und Druckdienste aus Samba 3 verwendet.

### Achtung

Bei der Verwendung von Samba 4 in einer verteilten Mehr-Server-Umgebung ist es zwingend erforderlich, dass alle Windows-Clients ihren jeweiligen Schul-DC als DNS-Server verwenden, um einen fehlerfreien Betrieb zu gewährleisten.

Bei Neuinstallationen von UCS@school wird standardmäßig Samba 4 empfohlen. Umgebungen, die von einer Vorversion aktualisiert wurden, können von Samba 3 auf Samba 4 migriert werden. Das dafür notwendige Vorgehen ist unter der folgenden URI dokumentiert:

http://wiki.univention.de/index.php?title=UCS%40school_Samba_3_to_Samba_4_Migration

Weiterführende Hinweise zur Konfiguration von Samba finden sich im UCS-Handbuch [ucs-handbuch].

## 7.2. Server für Dateifreigaben

Feedback

Beim Anlegen einer neuen Klasse bzw. eines Benutzers wird automatisch eine Klassenfreigabe für die Klasse bzw. eine Heimatverzeichnisfreigabe für den Benutzer eingerichtet. Der für die Einrichtung der Freigabe notwendige Dateiserver wird in den meisten Fällen ohne manuellen Eingriff bestimmt. Dazu wird am Schul-OU-Objekt bei der Registrierung einer Schule automatisch der in der Univention Management Console angegebene Schulserver als Dateiserver jeweils für Klassen- und Benutzerfreigaben hinterlegt.

Die an der Schul-OU hinterlegte Angabe bezieht sich ausschließlich auf neue Klassen- und Benutzerobjekte und hat keinen Einfluss auf bestehende Objekte im LDAP-Verzeichnis. Durch das Bearbeiten der entsprechenden Schul-OU im UMC-Modul *LDAP-Verzeichnis* können die Standarddateiserver für die geöffnete Schul-OU nachträglich modifiziert werden.

Es ist zu beachten, dass die an der Schul-OU hinterlegten Dateiserver nur in einer Multi-Server-Umgebung ausgewertet werden. In einer Single-Server-Umgebung wird für beide Freigabetypen beim Anlegen neuer Objekte immer der Domänencontroller Master als Dateiserver konfiguriert.

## 7.3. iTALC-Installation auf Windows-Clients

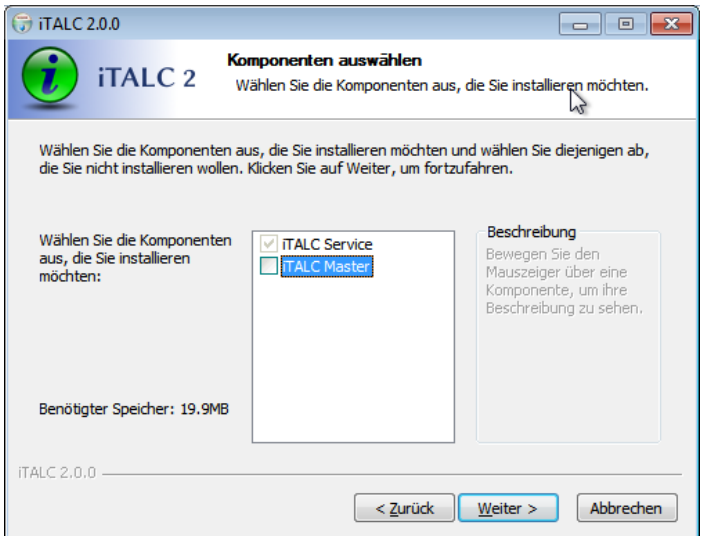
Feedback

Für die Kontrolle und Steuerung der Schüler-PCs integriert UCS@school optional die Software iTALC. Dieses Kapitel beschreibt die Installation von iTALC auf den Schüler-PCs. Die Administration durch die Lehrkräfte ist in der UCS@school-Lehrerdokumentation [ucs-school-teacher] beschrieben.

Für die Nutzung der Rechnerüberwachungs- und präsentationsfunktionen in der Computerraumverwaltung (siehe Abschnitt 4.1) wird vorausgesetzt, dass auf den Windows-Clients iTALC installiert wurde.

iTALC ist Open Source-Software und kann unter http://italc.sf.net/ heruntergeladen. Interoperabilitätstests zwischen UCS@school 3.1 und iTALC wurden ausschließlich mit der iTALC-Version 2.0 unter Windows XP und Windows 7 (32 und 64 Bit) durchgeführt.

### Abbildung 7.1. iTALC-Installation: Auswahl der Komponenten




iTALC bringt ein Installationsprogramm mit, das durch alle notwendigen Schritte führt. Während der Installation sollte nur der *iTALC Service* installiert und der *iTALC Master* abgewählt werden.

**Abbildung 7.2. iTALC-Installation: Babylon-Toolbar**


Die Babylon-Toolbar ist für die Funktion von UCS@school nicht notwendig und braucht daher nicht installiert zu werden.

Nach der Installation von iTALC auf dem Windows-Client muss der öffentliche Schlüssel importiert werden, damit der Schulserver Zugriff auf das installierte iTALC-Backend erhält. Dies erfolgt durch Aufruf der iTALC Management Console unter **Authentifizierung -> Schlüsseldatei-Assistent starten -> Öffentlichen Schlüssel importieren (Client-Computer) -> Lehrer**. Unter **Bitte geben Sie den Ort des öffentlichen Zugriffsschlüssels an, der importiert werden soll** ist der iTALC-Schlüssel des Schulservers anzugeben. Der Schlüssel wird automatisch auf der SYSVOL-Freigabe des Schulservers unter dem Namen der Schuldomäne unter `scripts` abgelegt (Kommt Samba 3 zum Einsatz, wird der Schlüssel auf der Netlogon-Freigabe abgelegt). Die Datei `italc-key.pub` muss in `italc-key.key.txt` umbenannt und kopiert werden, damit sie von dem Assistenten eingelesen werden kann.

Außerdem sollte auf den Windows-Clients sichergestellt werden, dass die installierte System-Firewall so konfiguriert ist, dass Port *11100* nicht blockiert wird. Dies ist Voraussetzung für eine funktionierende Umgebung, da iTALC diesen Port für die Kommunikation mit dem Schulserver bzw. anderen Computern verwendet.

# Kapitel 8. Web-Proxy auf den Schulservern

In der Grundeinstellung läuft auf jedem Schulserver (bzw. im Single-Server-Betrieb auf dem Domänencontroller Master) ein Proxy-Server auf Basis von Squid in Zusammenspiel mit Squidguard. Der Proxy erlaubt Lehrern in Schulstunden den Zugriff auf einzelne Webseiten zu beschränken oder auch generell bestimmte Webseiten zu sperren. Dies ist in der UCS@school-Lehrerdokumentation [ucs-school-teacher] beschrieben.

Der Proxyserver muss zwingend auf dem jeweiligen Schulserver betrieben werden.

Die Proxykonfiguration wird in der Grundeinstellung durch DHCP verteilt, diese Einstellung wird jedoch nicht von allen Browsern unterstützt. Die Konfiguration kann alternativ über eine Proxy-Autokonfigurationsdatei (PAC-Datei) automatisiert werden. In PAC-Dateien sind die relevanten Konfigurationparameter zusammengestellt. Die PAC-Datei eines Schulservers steht unter der folgenden URL bereit:

`http://schulserver.domaene.de/proxy.pac`

Im Internet Exlorer 8 wird die PAC-Datei beispielsweise unter **Internetoptionen -> Reiter Verbindungen -> LAN-Einstellungen -> Automatisches Konfigurationsskript verwendet** zugewiesen.

In Firefox 10 kann die PAC-Datei im Menü unter **Bearbeiten -> Einstellungen -> Erweitert -> Netzwerk -> Verbindungen -> Einstellungen -> Automatische Proxy-Konfigurations-URL** zugewiesen werden.

Bei Einsatz von Samba 4 kann die Proxy-Konfiguration alternativ auch über Gruppenrichtlinien zugewiesen werden.

# Kapitel 9. Authentifizierung des WLAN-Zugriffs über RADIUS



RADIUS ist ein Authentifizierungsprotokoll für Rechner in Computernetzen. Es wird in UCS@school für die Authentifizierung von Rechnern für den Wireless-LAN-Zugriff eingesetzt.

Der RADIUS-Server muss auf den Access Points konfiguriert werden. Die vom Client übertragenen Benutzerkennungen werden dann durch den festgelegten RADIUS-Server geprüft, der wiederum für die Authentifizierung auf den UCS-Verzeichnisdienst zugreift.

## 9.1. Installation und Konfiguration des RADIUS-Servers

Feedback

Um RADIUS-Unterstützung einzurichten muss das Paket ***ucs-school-radius-802.1x*** auf dem Schulserver der Schule installiert werden, in der WLAN-Authentifizierung eingerichtet werden soll. Außerdem muss das Paket ***ucs-school-webproxy*** auf dem Schulserver installiert sein.

Nun müssen alle Access Points der Schule in der Konfigurationsdatei `/etc/freeradius/clients.conf` registriert werden. Pro Access Point sollte ein zufälliges Passwort erstellt werden. Dies kann z.B. mit dem Befehl `makepasswd` geschehen. Die Kurzbezeichnung ist frei wählbar. Ein Beispiel für einen solchen Eintrag für einen Access Point:

```
client 192.168.100.101 {
    secret = a9RPAeVG
    shortname = AP01
}
```

## 9.2. Konfiguration der Access Points

Feedback

Nun müssen die Access Points konfiguriert werden. Die dafür nötigen Schritte unterscheiden sich je nach Hardwaremodell, prinzipiell müssen die folgenden vier Optionen konfiguriert werden:

- Der Authentifizierungmodus muss auf RADIUS-Authentifzierung umgestellt werden (diese Option wird oft auch als 'WPA Enterprise' bezeichnet)
- Die IP-Adresse des Schulservers muss als RADIUS-Server angegeben werden
- Der Radius-Port ist 1812 (sofern kein abweichender Port in Freeradius konfiguriert wurde)
- Das in der `/etc/freeradius/clients.conf` hinterlegte Passwort

## 9.3. Konfiguration der zugreifenden Clients

Feedback

Der zugreifende Client muss das SSL-Zertifikat des Radius-Servers importieren und eine Netzwerkverbindung mit den folgenden Parametern konfigurieren:

- Authentifizierung per WPA und TKIP als Verschlüsselungsverfahren

- PEAP und MSCHAPv2 als Authentifizierungsprotokoll

Die Konfiguration unterscheidet sich je nach Betriebsystem des Clients. Im Univention Wiki findet sich eine exemplarische Schritt-für-Schritt-Anleitung für die Einrichtung unter Windows XP: http://wiki.univention.de/index.php?title=Einrichtung-WLAN-Authentifizierung-WinXP.

## 9.4. Freigabe des WLAN-Zugriffs in der Univention Management Console

Feedback

In der Grundeinstellung ist der WLAN-Zugriff nicht zugelassen. Um einzelnen Benutzergruppen WLAN-Zugriff zu gestatten, muss in der Univention Management Console im Modul **Internetregeln definieren** eine Regel hinzugefügt - oder eine bestehende editiert werden -, in der die Option **WLAN-Authentifizierung aktiviert** aktiviert ist.

Weiterführende Dokumentation zur Freigabe des WLAN-Zugriffs finden sich in der UCS@school-Lehrerdokumentation [ucs-school-teacher].

## 9.5. Fehlersuche

Feedback

Im Fehlerfall sollte die Logdatei `/var/log/freeradius/radius.log` geprüft werden. Erfolgreiche Logins führen zu einem Logeintrag *Auth: Login OK* und eine fehlgeschlagene Authentifizierung beispielsweise zu *Auth: Login incorrect*.

univention
be open.

# Kapitel 10. Pre- und Post-Hook-Skripte für den Import



Während des Datenimports kann es notwendig sein, dass in Abhängigkeit von der jeweiligen Umgebung zusätzlich einige weitere Einstellungen vorgenommen werden müssen. Mit den Pre- und Post-Hook-Skripten besteht die Möglichkeit vor und nach dem Import eines Objektes, Skripte auszuführen. Zu allen Objekten und den davon jeweils unterstützten Operationen können mehrere Skripte definiert werden, die dann vor und nach den Operationen Anpassungen vornehmen.

Damit die Import-Skripte die Hook-Skripte finden können, müssen diese unterhalb des Verzeichnisses `/usr/share/ucs-school-import/hooks/` abgelegt werden. Dort gibt es für jede unterstützte Operation ein eigenes Unterverzeichnis. Beispielsweise gibt es das Verzeichnis `user_create_pre.d`, das alle Skripte enthalten muss, die vor dem Import eines Benutzers ausgeführt werden sollen. Alle weiteren Verzeichnisse sind nach dem gleichen Schema benannt: `<Objekt>_<Operation>_pre.d` für die Skripte, die *vor* einer Operation ausgeführt werden sollen und `<Objekt>_<Operation>_post.d` für die Skripte, die nach einer Operation ausgeführt werden sollen. Das Paket *ucs-school-import* bringt diese Verzeichnisse bereits mit. Skripte, die bei der Ausführung berücksichtigt werden sollen, müssen zwei Bedingungen erfüllen. Der Name darf nur aus Ziffern, Buchstaben und Unter- und Bindestrichen bestehen und die Ausführungsrechte müssen für die Datei gesetzt sein. Alle anderen Dateien in diesen Verzeichnissen werden ignoriert.

Die Hook-Skripte werden derzeit für die Objekttypen *ou*, *user*, *group*, *printer*, *computer*, *network* und *router* für die Operationen *create*, *modify* und *remove* ausgeführt. Dabei ist zu beachten, dass für Rechner (computer), Netzwerke, Router und Schul-OUs nur die Operation zum Erzeugen (create) definiert ist und daher auch nur dafür Hook-Skripte definiert werden können.

Die Pre-Hook-Skripte werden mit einem Parameter aufgerufen. Dieser enthält den Namen einer Datei in der die Zeile des als nächstes zu bearbeitenden Objektes aus der Import-Datei gespeichert ist. Darüber können die Skripte jede Einstellung für das Objekt auslesen; allerdings ist zu berücksichtigen, dass zu diesem Zeitpunkt die Daten noch nicht durch das Import-Skript geprüft worden sind. Die Post-Hook-Skripte bekommen als zusätzlichen Parameter noch den LDAP-DN des gerade bearbeiteten Objektes übergeben.

Das folgende Beispiel-Skript soll ausgeführt werden, nachdem eine neue Schul-OU angelegt wurde. Dafür muss das Skript in das Verzeichnis `/usr/share/ucs-school-import/hooks/ou_create_post.d/` kopiert werden. Die Aufgabe des Skriptes soll es sein, die LDAP-Basis für den DHCP-Server der Schule per Univention Configuration Registry-Richtlinie auf den Container *cn=dhcp* unterhalb der LDAP-Basis der Schule zu setzen.

```
#!/bin/sh
ldap_base="$(ucr get ldap/base)"
# Auslesen der ersten Spalte (OU-name) der Importdatei
ou="$(awk -F '\t' '{print $1}' "$1")"
# Den Standard-Schul-DC-Namen erzeugen
host="dc${ou}-01.$(ucr get domainname)"
# Eine UCR-Richtlinie erstellen und mit dem Schul-DC verbinden
udm policies/registry create \
  --position "cn=policies,ou=$ou,$ldap_base" \
  --set name=dhcpd_ldap_base \
  --append "registry=dhcpd/ldap/base=cn=dhcp,ou=$ou,$ldap_base"
```

```
udm computers/domaincontroller_slave \
  --dn "cn=dc${ou}-01,cn=dc,cn=computers,ou=$ou,$ldap_base" \
  --policy-reference "cn=dhcpd_ldap_base,cn=policies,ou=$ou,$ldap_base"
echo "$(basename $0): Added policy dhcpd_ldap_base ."
```

Obwohl das Skript `create_ou` keine Eingabedatei übergeben bekommt, wird für die Hook-Skripte eine generiert, die in der Zeile den Namen der OU enthält. Wenn ein vom Standard abweichender Schul-DC-Name angegeben wurde, wird dieser als zweiter Wert übergeben. Für alle anderen Operationen auf den Objekten können Hook-Skripte auf äquivalente Weise erstellt werden.

## 10.1. Erweiterung von Importdateien

Feedback

Eine weitere Funktion von den Hook-Skripten ist die Möglichkeit mit Erweiterungen in den Import-Dateien umzugehen, d.h. wenn in den Importdateien mehr Felder eingetragen sind, als durch die Import-Skripte selbst verarbeitet werden, so können die erweiterten Attribute in den Hook-Skripten ausgelesen und verarbeitet werden. Als Beispiel könnten bei den Benutzern Adressinformationen oder eine Abteilung gespeichert werden. Die zusätzlichen Felder werden in den Importdateien jeweils hinten an die Zeilen getrennt durch einen Tabulator angehängt. Da die Hook-Skripte die komplette Zeile übergeben bekommen, kann ein Post-Hook Skript genutzt werden, um die neuen Felder auszulesen und die Informationen z.B. an dem gerade erzeugten Benutzer zu ergänzen.

## 10.2. Beispiel-Hook-Skript: automatische Erstellung der Marktplatzfreigabe

Feedback

Um den Austausch von Dokumenten zwischen Benutzern zu erleichtern, wird empfohlen, die Freigabe *Marktplatz* auf den jeweiligen Schul-DCs anzulegen, auf die alle Benutzer Zugriff erhalten.

Das Hookskript `ou_create_post.d/52marktplatz_create` wird ab UCS@school für UCS 2.4 mitgeliefert und legt beim Aufruf von `create_ou` die Freigabe ``Marktplatz'' automatisch an. Über die Univention Configuration Registry-Variable `ucsschool/import/generate/share/marktplatz` kann der Hook de-/aktiviert werden, indem der Variable der Wert *no* bzw. *yes* zugeordnet wird.

Über drei weitere Univention Configuration Registry-Variablen kann das Verhalten des Hooks gesteuert werden:

- `ucsschool/import/generate/share/marktplatz/sharepath`

  Diese Variable definiert das Verzeichnis auf dem Server, welches als Freigabe *Marktplatz* freigegeben wird. In der Standardeinstellung wird das Verzeichnis `/home/groups/Marktplatz` verwendet.

- `ucsschool/import/generate/share/marktplatz/group`

  Beim Anlegen der Freigabe wird die in dieser Variable definierte Gruppe als Gruppenbesitzer der Freigabe festgelegt. In der Standardeinstellung ist dies die Gruppe *Domain Users*. Es ist zu beachten, dass abweichend vom UCS-Standard die über die Importskripte angelegten Benutzer nicht in der Gruppe *Domain Users* enthalten sind.

- `ucsschool/import/generate/share/marktplatz/permissions`

  Die Zugriffsrechte der Freigabe sind in oktaler Schreibweise anzugeben (z.B. 0777). In der Standardeinstellung erhalten der Benutzer *root*, die vordefinierte Gruppe (z.B. *Domain Users*) sowie alle sonstigen Benutzer Lese- und Schreibrechte (0777).

## 10.3. Beispiel-Hook-Skript: Setzen des LDAP-Containers für DHCP-Objekte



Auf den Schul-DCs wird ein abweichender Container für DHCP-Objekte verwendet, weshalb die Univention Configuration Registry-Variable `dhcpd/ldap/base` entsprechend gesetzt werden muss. Um das manuelle Setzen der UCR-Variable für jede neue OU bzw. jeden neuen Schul-DC zu vermeiden, wird über den Standard-Hook `ou_create_post.d/40dhcpsearchbase_create` automatisch beim Erstellen einer OU die UCR-Richtlinie *ou-default-ucr-policy* im Container *cn=policies,ou=XXX,LDAPBASIS* angelegt und anschließend mit dem OU-Objekt *ou=XXX,LDAPBASIS* verknüpft. Über die Richtlinie wird die Univention Configuration Registry-Variable `dhcpd/ldap/base` entsprechend gesetzt. Dadurch wird sichergestellt, dass die in der Richtlinie gesetzten UCR-Variablen auf allen UCS-Systemen der OU automatisch übernommen werden.

# Literaturverzeichnis

[ucs-handbuch] Univention GmbH. 2013. *Univention Corporate Server - Handbuch für Benutzer und Administratoren*. http://docs.univention.de/handbuch-3.1-1.pdf.

[ucs-school-teacher] Univention GmbH. 2013. *UCS@school - Handbuch für Lehrkräfte und Schuladministratoren*. http://docs.univention.de/ucsschool-lehrer-handbuch.html.