

# UCS@school



**Handbuch für Administratoren**

Version 3.1 R2-2  
Stand: 07. Oktober 2013

Alle Rechte vorbehalten./ All rights reserved.  
(c) 2002-2013  
Univention GmbH  
Mary-Somerville-Straße 1  
28359 Bremen  
Deutschland  
feedback@univention.de

Jede aufgeführte Marke und jedes Warenzeichen steht im Eigentum ihrer jeweiligen eingetragenen Rechtsinhaber. Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case. Linux is a registered trademark of Linus Torvalds.

## Inhaltsverzeichnis

1. Einführung .....	5
2. Aufbau einer UCS@school-Umgebung .....	7
2.1. UCS@school-Benutzerrollen .....	7
2.2. Aufteilung von UCS@school .....	7
2.2.1. Replikation der LDAP-Daten auf die Schul-Standorte .....	8
2.3. Verwaltungsnetz und Edukativnetz .....	8
3. Installation .....	11
3.1. Installation einer Single-Server-Umgebung .....	11
3.1.1. Installation des DC Master .....	11
3.2. Installation einer Multi-Server-Umgebung .....	12
3.2.1. Installation des DC Master .....	12
3.2.2. Installation eines DC Backup (optional) .....	13
3.2.3. Installation eines Schulserver .....	13
3.2.4. Installation eines Verwaltungsservers .....	14
3.3. Domänenbeitritt eines Schulservers .....	14
3.4. Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung .....	15
4. Übersicht über die schulspezifischen Anwendungen .....	17
4.1. Modulübersicht .....	17
5. Einrichtung einer Schule .....	19
5.1. Registrierung einer Schule .....	19
5.2. Import von Benutzerkonten .....	19
5.3. Skriptbasierter Import von Netzwerken .....	19
5.4. Import von Rechnerkonten für Windows-PCs .....	20
5.4.1. Anlegen einzelner PCs .....	20
5.4.2. Skriptbasierter Import von PCs .....	21
5.5. Konfiguration von Druckern an der Schule .....	21
5.5.1. Einrichtung der Druckmoderation .....	22
5.5.2. Anlegen eines PDF-Druckers für die Druckermoderation .....	23
5.6. Anlegen von Freigaben .....	23
5.7. Konfiguration der Helpdesk-Kontaktadresse .....	23
6. Verwaltung von Schüler-, Lehrer- und Mitarbeiterdaten .....	25
6.1. Import von Benutzerkonten für Schüler, Lehrer und Mitarbeiter .....	25
6.1.1. Windows-spezifische Benutzereinstellungen .....	27
6.1.2. Manuelles Anlegen von Benutzerkonten für Mitarbeiter .....	28
6.1.3. Anlegen von Benutzerkonten für Schuladministratoren .....	28
6.2. Skriptgesteuerter Import von Klassen .....	28
6.3. Vorgehen zum Schuljahreswechsel .....	29
7. Integration und Verwaltung von Microsoft Windows-Clients .....	31
7.1. Anmeldedienste mit Samba .....	31
7.2. Server für Dateifreigaben .....	32
7.3. Netlogon-Skripte für Samba4-Umgebung .....	32
7.4. iTALC-Installation auf Windows-Clients .....	33
8. Web-Proxy auf den Schulservern .....	35
9. Authentifizierung des WLAN-Zugriffs über RADIUS .....	37
9.1. Installation und Konfiguration des RADIUS-Servers .....	37
9.2. Konfiguration der Access Points .....	37
9.3. Konfiguration der zugreifenden Clients .....	37
9.4. Freigabe des WLAN-Zugriffs in der Univention Management Console .....	38
9.5. Fehlersuche .....	38
10. Pre- und Post-Hook-Skripte für den Import .....	39
10.1. Erweiterung von Importdateien .....	40
10.2. Beispiel-Hook-Skript: automatische Erstellung der Marktplatzfreigabe .....	40

10.3. Beispiel-Hook-Skript: Setzen des LDAP-Containers für DHCP-Objekte .....	41
11. Klassenarbeitsmodus .....	43
11.1. Technische Hintergründe .....	43
11.2. Konfiguration .....	44
11.3. Beispiele für Gruppenrichtlinien .....	45
11.3.1. Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen .....	46
11.3.2. Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken .....	46
11.3.2.1. Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken.....	46
11.3.2.2. Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer .....	47
11.3.3. Zugriff auf USB-Speicher und Wechselmedien einschränken .....	48
11.3.3.1. Zugriff auf USB-Speicher an Windows XP einschränken .....	48
11.3.3.2. Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten .....	48
11.3.3.3. Zugriff auf USB-Speicher an Windows 7 einschränken .....	49
11.3.3.4. Installation neuer Gerätetreiber für USB-Speicher an Windows 7 Clients verbieten .....	49
11.3.4. Vorgabe von Proxy-Einstellungen für den Internetzugriff .....	50
11.3.4.1. Proxy-Vorgabe für den Internet Explorer .....	50
11.3.4.2. Sperrung der Proxyeinstellung für den Internet Explorer .....	50
11.3.4.3. Proxy-Vorgabe für Google Chrome .....	50
11.3.4.4. Proxy-Vorgabe für Mozilla Firefox .....	51
11.3.5. Zugriff auf bestimmte Programme einschränken .....	52
11.3.5.1. Kommandoingabeaufforderung deaktivieren .....	52
11.3.5.2. Zugriff auf Windows-Registry-Editor deaktivieren .....	52
11.3.5.3. Konfiguration von Software Restriction Policies (SRP) .....	53
12. Integration und Verwaltung von Univention Corporate Client-Systemen .....	55
12.1. Installation von UCC .....	56
12.2. Konfigurationseinstellungen für UCC-Systeme .....	56
12.3. Ausrollen von neuen UCC-Systemen .....	57
Literaturverzeichnis .....	59

# 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 Domänenendaten (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

2.1. UCS@school-Benutzerrollen .....	7
2.2. Aufteilung von UCS@school .....	7
2.2.1. Replikation der LDAP-Daten auf die Schul-Standorte .....	8
2.3. Verwaltungsnetz und Edukativnetz .....	8

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

Feedback 


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

Feedback 


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.

## Achtung

UCS@school unterstützt derzeit nur einen Schulserver pro Standort. Darüber hinaus können regulär weitere UCS-Systeme ohne Samba 4 installiert und an den Schul-Standorten betrieben werden. Diese zusätzlichen UCS-Systeme können jedoch nicht in Verbindung mit UCS@school-Funktionalitäten eingesetzt werden; z.B. wird das Sperren von Dateifreigaben über die UCS@school-UMC-Module auf den zusätzlichen UCS-Systemen nicht unterstützt. Zusätzlich müssen die Rechnerobjekte der zusätzlichen UCS-Systeme vor dem Domänenbeitritt unterhalb der Organisationseinheit (OU) der Schule angelegt werden (siehe auch Abschnitt 2.2.1).

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


Feedback 

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 *340* oder zusammengesetzte Kürzel wie *g123m* oder *gymmitte* zum Einsatz.

### 2.3. Verwaltungsnetz und Edukativnetz

Feedback 

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. Diese Server verwenden für ihre Client-Systeme (Schülerrechner bzw. Rechner der Verwaltung) jeweils ein eigenes IP-Subnetz.

Auch bei der Unterteilung in Verwaltungsnetz und Edukativnetz findet eine selektive Replikation statt, wie sie in Abschnitt 2.2.1 beschrieben wird. Zusätzlich wird jedoch bei der Replikation der Benutzerkonten anhand ihrer Benutzerrolle(n) unterschieden. Auf den Schulserver des edukativen Netzes werden die Benutzerkonten mit den Benutzerrollen *Schüler*, *Lehrer*, *Schuladministrator* und *System-Administrator* repliziert. Auf den Schulserver der Verwaltung werden die Benutzerkonten mit den Benutzerrollen *Mitarbeiter*, *Schuladministrator* und *System-Administrator* repliziert. Die gemeinsame Verwendung der Benutzerrollen *Lehrer* und *Mitarbeiter* für ein Benutzerkonto ist möglich, z.B. für Benutzerkonten der Schulleitung, die neben ihrer Verwaltungstätigkeit auch lehrend tätig sind.

Auf den Schulservern des Verwaltungsnetzes werden keine speziellen Dienste oder UMC-Module angeboten. Sie dienen den Verwaltungsrechnern hauptsächlich als Anmelde-, Druck- und Dateiserver. Die Benutzerkon-



ten mit der Benutzerrolle *Mitarbeiter* haben entsprechend keinen Zugriff auf die UCS@school-spezifischen UMC-Module des edukativen Netzes.

### **Achtung**

Voraussetzung für diese Unterteilung ist eine physikalische Trennung der beiden Netzwerksegmente. D.h. das edukative Netz und das Verwaltungsnetz können nicht gleichzeitig im gleichen Netzwerksegment verwendet werden.




## Kapitel 3. Installation

3.1. Installation einer Single-Server-Umgebung .....	11
3.1.1. Installation des DC Master .....	11
3.2. Installation einer Multi-Server-Umgebung .....	12
3.2.1. Installation des DC Master .....	12
3.2.2. Installation eines DC Backup (optional) .....	13
3.2.3. Installation eines Schulserver .....	13
3.2.4. Installation eines Verwaltungsservers .....	14
3.3. Domänenbeitritt eines Schulservers .....	14
3.4. Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung .....	15


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-Umgebung und die Installation als Multi-Server-Umgebung mit einem Domänencontroller Master und mindestens einem Schulserver. Die nachträgliche Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung wird unterstützt und in Abschnitt 3.4 genauer beschrieben.

### 3.1. Installation einer Single-Server-Umgebung

Feedback 

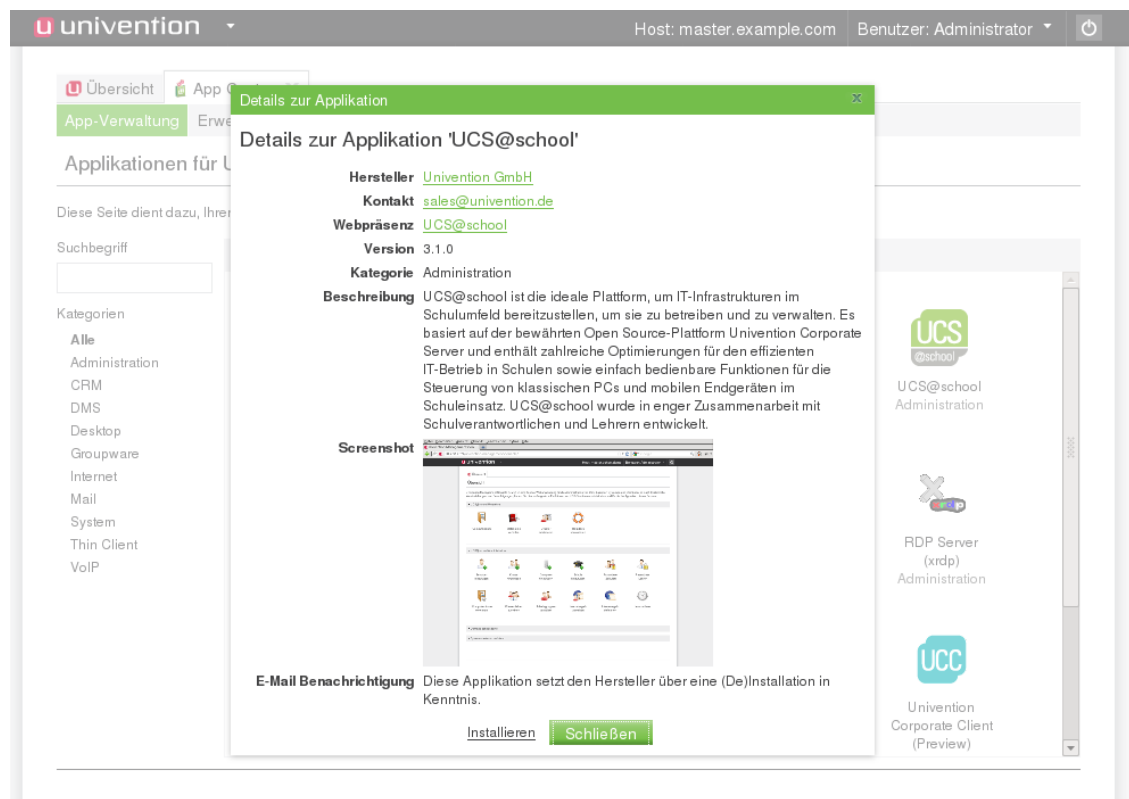
#### 3.1.1. Installation des DC Master

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-Umgebung* 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. *schule340* 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 Konfiguration der Schule vorgenommen werden, siehe Kapitel 5.

## 3.2. Installation einer Multi-Server-Umgebung

 Feedback 

### 3.2.1. Installation des DC Master

 Feedback 

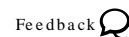
Bei der UCS-Installation muss die Systemrolle *Domänencontroller Master* ausgewählt werden. Nach der UCS-Installation kann in Univention Management Console das Modul **App Center** geöffnet und dort die Applikation *UCS@school* nachinstalliert werden. Nach Abschluss der Installation wird in Univention Management Console ein neues Modul 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 *Multi-Server-Umgebung* auszuwählen.
- Weitere Konfigurationsoptionen werden in einer Multi-Server-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)



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

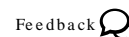
Ein DC Backup dient als Fallback-System des DC Master. Sollte dieser ausfallen, kann ein DC Backup die Rolle des DC Master dauerhaft übernehmen. Der Einsatz eines DC Backup ist optional.

Die Installation von UCS@school auf einem DC Backup erfolgt analog zur in Abschnitt 3.2 beschriebenen Installation des DC Master.

#### Achtung

Sofern DC Backup-Systeme in der UCS-Domäne vorhanden sind, muss dort ebenfalls UCS@school installiert und konfiguriert werden. Sollte dies nicht der Fall sein, kann es zu Replikationsproblemen auf den Schulservern kommen.

### 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 beitrifft. 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. *schule340* 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.

Wurde während der Installation des DC Slaves ein DHCP-Server installiert, verschiebt der UCS@school-Konfigurationsassistent das DHCP-Server-Objekt des DC Slaves (zu finden unter *cn=dhcp, LDAPBASIS*) automatisch in den entsprechenden DHCP-Container der OU (*cn=dhcp, ou=OUNAME, LDAPBASIS*). Dies ist es für die korrekte Funktion des DHCP-Servers notwendig, da jeder Schulserver eine individuelle LDAP-Suchbasis verwendet.

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

### 3.2.4. Installation eines Verwaltungsservers

 Feedback 


Bei einem UCS@school-Verwaltungsserver handelt es sich genau wie beim Schulserver um ein UCS-System mit der Systemrolle *Domänencontroller Slave*. Das System ist wie ein Standard-UCS-DC Slave zu installieren. Nach Abschluss der regulären UCS-Installation müssen alle verfügbaren UCS-Errata eingespielt und das UCS@school-Paket *ucs-school-nonedu-slave* installiert werden. Dies kann auf der Kommandozeile über die beiden folgenden Befehle erfolgen:

```
univention-upgrade
univention-add-app --latest ucsschool ucs-school-nonedu-slave
```

#### Achtung

Bei der Installation des Systems ist zu beachten, dass für den Verwaltungsserver ein vom edukativen Netz physikalisch getrenntes Netzwerksegment sowie ein eigenes IP-Subnetz verwendet wird, um Konflikte mit dem Schulserver des Edukativnetzes zu vermeiden (siehe auch Abschnitt 2.3).

### 3.3. Domänenbeitritt eines Schulservers

 Feedback 

Die Einrichtung eines Schulservers ist auch ohne das oben beschriebene UMC-Konfigurationsmodul möglich, bzw. notwendig, wenn während des Konfigurationsprozesses 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).

#### Achtung

Wird auf dem Schulserver Samba 4 eingesetzt, ist es notwendig, vor dem erneuten Domänenbeitritt als Benutzer *root* die folgenden zwei Befehle auszuführen, um spätere Probleme mit dem Samba 4-Dienst zu vermeiden:

```
mv /var/lib/samba/private /var/lib/samba/private.BACKUP
mkdir -p /var/lib/samba/private
```

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.

#### Anmerkung

Der Name des Schulservers darf nur aus Kleinbuchstaben, Ziffern sowie dem Bindestrich bestehen (a-z, 0-9 und -). Der Name darf nur mit einem Kleinbuchstaben beginnen, mit einem Kleinbuchstaben oder einer Ziffer enden und ist auf eine Länge von 12 Zeichen beschränkt. Bei Abweichungen von diesen Vorgaben kann es zu Problemen bei der Verwendung von Windows-Clients kommen.

## 3.4. Umwandlung einer Single-Server-Umgebung in eine Multi-Server-Umgebung Feedback

UCS@school-Umgebungen, die als Single-Server-Umgebung installiert/ingerichtet wurden, können bei Bedarf nachträglich in eine Multi-Server-Umgebung umgewandelt werden. Die Umwandlung ermöglicht die Aufnahme von Schulservern in die Domäne.

Für die Umwandlung sind einige Befehle auf der Kommandozeile des DC Masters auszuführen, die einen Austausch des UCS@school-Metapakets sowie eine Konfigurationsänderung durchführen (Bitte das Minuszeichen hinter dem zweiten Paketnamen beachten):

```
univention-install ucs-school-master ucs-school-singlemaster-  
ucr unset ucsschool/singlemaster
```

Mit der Deinstallation des Pakets *ucs-school-singlemaster* werden die nachfolgenden UCS@school-spezifischen Pakete (UMC-Module), die normalerweise nicht auf einem DC Master der Multi-Server-Umgebung installiert sind, automatisch zur Löschung vorgesehen. Die eigentliche Löschung findet während des nächsten Updates oder durch den manuellen Aufruf von `apt-get autoremove` statt. Dabei ist zu beachten, dass neben den genannten Paketen ggf. auch ungenutzte Paketabhängigkeiten entfernt werden.

```
ucs-school-branding  
ucs-school-umc-computerroom  
ucs-school-umc-distribution  
ucs-school-umc-exam  
ucs-school-umc-helpdesk  
ucs-school-umc-internetrules  
ucs-school-umc-lessontimes  
ucs-school-umc-printermoderation  
ucs-school-webproxy
```

Um die Löschung einzelner Pakete zu vermeiden, kann der folgende Befehl verwendet werden, bei dem `PAKETNAME` durch den gewünschten Paketnamen auszutauschen ist:

```
apt-get unmarkauto PAKETNAME
```

Richtlinien, die (ggf. automatisch von UCS@school) an Container der Schul-OU's verknüpft wurden, sollte auf ihre Einstellungen hin überprüft werden. Dies betrifft unter anderem die DHCP-DNS-Einstellungen sowie die Einstellungen für UCC-Systeme (siehe auch Abschnitt 12.2).

Nachdem die oben genannten Schritte ausgeführt wurden, sollte abschließend der UMC-Server auf dem DC Master neu gestartet werden:

```
invoke-rc.d univention-management-console-server restart
```

### Achtung

Es ist zu beachten, dass auch nach der abgeschlossenen Umwandlung in eine Multi-Server-Umgebung der auf dem DC Master installierte Samba3- oder Samba4-Dienst bestehen bleibt und nicht automatisch deinstalliert wird.

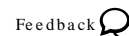




# Kapitel 4. Übersicht über die schulspezifischen Anwendungen

4.1. Modulübersicht ..... 17

## 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 Bildschirminhalt 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 und Lehrer in klassenübergreifende Arbeitsgruppen einzuordnen.

Das Anlegen einer Arbeitsgruppe legt automatisch einen Datenbereich auf dem Schulserver (Dateifreigabe) an, auf den alle Mitglieder der Arbeitsgruppe Zugriff erhalten. Der Name der Dateifreigabe ist identisch mit dem gewählten Namen der Arbeitsgruppe.

Das Anlegen, Bearbeiten und Löschen von Arbeitsgruppen ist in der Standardkonfiguration sowohl den Lehrern als auch den Schuladministratoren erlaubt.

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

## Modulübersicht

- 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 .....	19
5.2. Import von Benutzerkonten .....	19
5.3. Skriptbasierter Import von Netzwerken .....	19
5.4. Import von Rechnerkonten für Windows-PCs .....	20
5.4.1. Anlegen einzelner PCs .....	20
5.4.2. Skriptbasierter Import von PCs .....	21
5.5. Konfiguration von Druckern an der Schule .....	21
5.5.1. Einrichtung der Druckmoderation .....	22
5.5.2. Anlegen eines PDF-Druckers für die Druckermoderation .....	23
5.6. Anlegen von Freigaben .....	23
5.7. Konfiguration der Helpdesk-Kontaktadresse .....	23

## 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. *schule340* oder *gymnasium\_mitte*. In Single-Server-Umgebungen ist die Angabe eines Schulservernamens nicht erforderlich, während in Multi-Server-Umgebungen der **Rechnername des Schulservers** angegeben werden muss. 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.

### Anmerkung

Der Schulname darf nur aus Groß- und Kleinbuchstaben sowie Ziffern und dem Unterstrich bestehen (A-Z, a-z, 0-9 und   ) und nicht mit dem Unterstrich beginnen oder enden.


Der Name des Schulservers darf nur aus Kleinbuchstaben, Ziffern sowie dem Bindestrich bestehen (a-z, 0-9 und -). Der Name darf nur mit einem Kleinbuchstaben beginnen, mit einem Kleinbuchstaben oder einer Ziffer enden und ist auf eine Länge von 12 Zeichen beschränkt. Bei Abweichungen von diesen Vorgaben kann es zu Problemen bei der Verwendung von Windows-Clients kommen.

## 5.2. Import von Benutzerkonten

Feedback 

Der Import der Schüler-, Lehrer- und Mitarbeiterdaten erfolgt in der Regel an zentraler Stelle durch Schulträger. Der skriptbasierte Import von Benutzerkonten wird in Kapitel 6 beschrieben.

## 5.3. Skriptbasierter Import von Netzwerken

Feedback 

Durch den Import von Netzwerken können IP-Subnetze im LDAP angelegt werden und diverse Voreinstellungen wie Adressen von Router, DNS-Server etc. für diese Subnetze konfiguriert werden. Darunter fällt z.B. auch ein Adressbereich aus dem für neuangelegte Systeme automatisch IP-Adressen vergeben werden können.

## Import von Rechnerkonten für Windows-PCs

Das Importieren von Subnetzen empfiehlt sich in größeren UCS@school-Umgebungen. Kleinere Umgebungen können diesen Schritt häufig überspringen, da fehlende Netzwerke beim Import von Rechnerkonten automatisch angelegt werden.

Netzwerke können derzeit nur auf der Kommandozeile 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	g123m
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:

```
g123m 10.0.5.0 10.0.5.1 10.0.5.2 10.0.5.2
g123m 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`.


## 5.4. Import von Rechnerkonten für Windows-PCs

Feedback 

Rechnerkonten können entweder einzeln über ein spezielles UMC-Modul oder über ein spezielles Import-Skript als Massenimport angelegt werden. Die Rechnerkonten sollten vor dem Domänenbeitritt von z.B. Windows-PCs angelegt werden, da so sichergestellt wird, dass die für den Betrieb von UCS@school notwendigen Informationen im LDAP-Verzeichnis vorhanden sind und die Objekte an der korrekten Position im LDAP-Verzeichnis abgelegt wurden.

Nach dem Anlegen der Rechnerkonten können Windows-PCs über den im UCS-Handbuch beschriebenen Weg der Domäne beitreten.


### 5.4.1. Anlegen einzelner 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. Wurde mehr als eine Schule im LDAP-Verzeichnis angelegt, ist zunächst die gewünschte Schule auszuwählen. Anschließend stehen zwei Rechnertypen 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 wird unter anderem für die Vergabe der IP-Adressen per DHCP verwendet.

## 5.4.2. Skriptbasierter Import von PCs

 Feedback 

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. `340win01` für Schule 340).

Feld	Beschreibung	Mögliche Werte	Beispiel
Rechnertyp	Typ des Rechnerobjektes	ipmanagedclient, macos, ucc, windows	windows
Name	Zu verwendender Rechnername	---	wing123m-01
MAC-Adresse	MAC-Adresse (wird für DHCP benötigt)	---	00:0c:29:12:23:34
OU	OU, in der das Rechnerobjekt modifiziert werden soll	---	g123m
IP-Adresse (/ Netzmaske) oder IP-Subnetz	IP-Adresse des Rechnerobjektes und optional die passende Netzmaske; alternativ das Ziel-IP-Subnetz	---	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 IP-Subnetz zugewiesen.

Beispiel für eine Importdatei:

```
ipmanagedclient  routerg123m-01  10:00:ee:ff:cc:02  g123m  10.0.5.1
windows          wing123m-01  10:00:ee:ff:cc:00  g123m  10.0.5.5
windows          wing123m-02  10:00:ee:ff:cc:01  g123m  10.0.5.6
macos            macg123m-01  10:00:ee:ff:cc:03  g123m  10.0.5.7
ipmanagedclient  printerg123m-01  10:00:ee:ff:cc:04  g123m  10.0.5.250
ucc              uccg123m-01  10:00:ee:ff:cd:e2  g123m  10.0.5.10
```

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.

## 5.5. 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` aufge-

rufen 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 Druckermodifikation	A=Hinzufügen, M=Modifizieren, D=Löschen	A
OU	OU, in der das Druckerobjekt modifiziert werden soll	---	g123m
Druckserver	Name des zu verwendenen Druckservers	---	dcg123m-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.

## 5.5.1. Einrichtung der Druckmoderation

Feedback 

Um unnötige oder fehlerhafte Druckaufträge zu minimieren, bietet UCS@school den Lehrern die Möglichkeit, Druckaufträge zu moderieren. Dafür werden die Druckaufträge zunächst über einen speziellen PDF-Drucker (Druckerfreigabe *PDFDrucker*) auf dem Schüler-/Lehrerrechner gedruckt und anschließend durch den Lehrer im UMC-Modul *Drucker moderieren* betrachtet, verworfen oder für den Druck freigegeben.

In UCS@school gibt es vielfältige Möglichkeiten die Druckmoderation zu konfigurieren und einzusetzen. Nachfolgend wird die Einrichtung eines einzelnen Szenarios beschrieben, welches leicht an die Bedürfnisse der eigenen Schulumgebung angepasst werden kann. In dem beschriebenen Szenario wird der Zugriff auf die physikalischen Drucker für alle Schüler gesperrt.


Für die Druckmoderation ist es erforderlich, dass zunächst wie in Abschnitt 5.5 beschrieben, Druckfreigaben für die zu verwendenden, physikalisch existierenden Drucker angelegt werden.

An den Druckerfreigabeobjekten (UMC-Modul *Drucker*) können spezielle Zugriffsrechte gesetzt werden. Dabei kann der Zugriff für einzelne Benutzer oder ganze Gruppen erlaubt bzw. gesperrt werden. Um den Schülern den Zugriff auf die physikalischen Drucker zu verbieten, muss an den Druckerfreigaben für diese Drucker der Zugriff durch Benutzer der ou-spezifischen Gruppe *schueler-OU* (z.B. *schueler-gsmittle*) verboten werden. Für den PDF-Drucker *PDFDrucker* sollten keine Einschränkungen gemacht werden.

Schüler haben damit nur noch die Möglichkeit Druckaufträge an den *PDFDrucker* zu senden. Im UMC-Modul *Drucker moderieren* können die Druckaufträge anschließend durch den Lehrer aufgelistet und betrachtet werden. Dafür ist ein geeignetes Programm zur Anzeige von PDF-Dateien auf den Lehrerrechnern erforderlich. Die Druckaufträge können dann durch den Lehrer an einen beliebigen physikalischen Drucker der Schule weitergeleitet oder auch verworfen werden.

Um Ausnahmen von dieser strikte Regelung zu ermöglichen, kann der Lehrer im UMC-Modul *Computerraum* über den Punkt *Einstellungen ändern* den Druckmodus für einen einzelnen Computerraum beeinflussen. Die oben beschriebenen Einschränkungen für Schüler werden dabei als *Standard (globale Einstellungen)* beschrieben. Darüber hinaus können auch die Druckmodi *Drucken deaktiviert* und *Drucken möglich* ausgewählt werden, die das Drucken von den Rechnern des Computerraums entweder vollständig untersagen oder - unabhängig der gemachten Voreinstellungen - auf allen physikalischen Druckern erlauben.

## 5.5.2. 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 unterhalb der OU der Schule angelegt werden. Dies geschieht in der Regel automatisch bei der Installation von UCS@school bzw. dem Ausführen der Joinskripte.

Sollte der PDF-Drucker für eine OU fehlen, gibt es zwei Möglichkeiten dieses für eine OU zu erstellen:

- Auf dem Schulserver kann über das UMC-Modul *Domänenbeitritt* das Joinskript *80ucs-school-umc-printermoderation* (erneut) ausgeführt werden.
- Alternativ kann das LDAP-Objekt im zuständigen Container für Druckerfreigaben der betreffenden OU (siehe oben) angelegt werden. Dabei müssen folgende Werte am Druckerfreigabe-Objekt gesetzt werden:
  - **Server** : Name des Schulservers
  - **Protokoll** : *cups-pdf:/*
  - **Ziel** : leer
  - **Drucker-Hersteller** : *PDF*
  - **Drucker-Modell** : *Generic CUPS-PDF Printer*

## 5.6. 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/marktplatz` 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. Für die OU *gym17* muss beispielsweise der Container *gym17/shares* ausgewählt werden.

## 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

*Konfiguration der Helpdesk-Kontaktadresse*


Registry-Variable `ucsschool/helpdesk/recipient` auf die E-Mail-Adresse des zuständigen Helpdesk-Teams gesetzt werden.



# Kapitel 6. Verwaltung von Schüler-, Lehrer- und Mitarbeiterdaten

6.1. Import von Benutzerkonten für Schüler, Lehrer und Mitarbeiter .....	25
6.1.1. Windows-spezifische Benutzereinstellungen .....	27
6.1.2. Manuelles Anlegen von Benutzerkonten für Mitarbeiter .....	28
6.1.3. Anlegen von Benutzerkonten für Schuladministratoren .....	28
6.2. Skriptgesteuerter Import von Klassen .....	28
6.3. Vorgehen zum Schuljahreswechsel .....	29

## 6.1. Import von Benutzerkonten für Schüler, Lehrer und Mitarbeiter

Feedback 

Die Verwaltung der Schüler-, Lehrer und Mitarbeiterdaten 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- und Multi-Server-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
Benutzerna- me	Der zum Login verwendete Benutzerna- me	---	m.mustermann
Nachname	Der Nachname des Benutzers	---	Mustermann
Vorname	Der Vorname des Benutzers	---	Michael
OU	Die OU, unter der der Benutzer angelegt werden soll	---	g123m
Klasse	Name der Klasse des Benutzers; nur Lehrer können in mehreren Klassen ver- treten sein!	---	1A,1B,2A,4C
Rechte	derzeit ungenutzt; das Feld sollte leer bleiben, so dass 2 Tabulator-Zeichen aufeinander folgen	---	

Import von Benutzerkonten für Schüler, Lehrer und Mitarbeiter

Feld	Beschreibung	Mögliche Werte	Beispiel
Email-Adresse	Mailadresse des Benutzers	---	m.musterm@beispiel.edu
(Lehrer)	Definiert, ob der Benutzer ein Lehrer ist	0=Kein Lehrer, 1=Lehrer	1
(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	g123m	1A	max@schule.edu	0	1	0
M	m.musterma	Mustermann	Moritz	g123m	1A, 2D, 4C	m.m@schule.edu	1	1	0
D	a.musterfr	Musterfrau	Anke	g123m	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. Bei Mitarbeitern ist das Feld *Klasse* leer zu lassen.

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 zufälligen, unbekanntenen Passwörtern initialisiert. Mehrere Personengruppen können die Konten anschließend freischalten:

- Das Konto eines Schuladministrators kann durch Benutzer der Gruppe *Domain Admins* in der Univention Management Console erstellt und modifiziert werden.
- Die Konten von Mitarbeitern können durch Benutzer der Gruppe *Domain Admins* in der Univention Management Console durch die Vergabe eines Passworts freigeschaltet werden.
- Die Konten von Lehrern können durch den Schuladministrator über das Modul **Passwörter (Schüler)** durch die Vergabe eines Passworts freigeschaltet werden.
- Die Konten von Schülern können durch Lehrer über das Modul **Passwörter (Lehrer)** klassenweise durch die 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.

## Achtung

Bei der Verwendung von Samba 4 benötigt der S4-Connector einige Zeit, um die Benutzer in die Samba 4-Benutzerdatenbank zu synchronisieren. Je nach Menge der Importdaten und der verwendeten Hardware kann die Synchronisation einige Stunden benötigen. Währenddessen kann es zu Verzögerungen in der Synchronisation von nicht-import-abhängigen Änderungen im LDAP oder Active Directory kommen (z.B. interaktive Änderung von Benutzerpasswörtern).

### 6.1.1. Windows-spezifische Benutzereinstellungen

Feedback 

Neben den in Abschnitt 6.1 genannten Attributen für Benutzer werden beim Anlegen eines Benutzers auch automatisch einige Windows-spezifische Einstellungen vorgenommen:

- Für die Verwendung von Samba ist es notwendig, dass für jeden Benutzer ein Pfad für das Windows-Benutzerprofil vorgegeben wird. In der Standardeinstellung von UCS@school wird der jeweilige Logonserver als Ablageort für das Benutzerprofil definiert (`\\%LOGONSERVER%%\%USERNAME%\windows-profiles\default`). Falls die Benutzerprofile abweichend auf einem anderen Dateiserver gespeichert werden sollen, kann in der Univention Management Console am Rechnerobjekt des gewünschten Dateiservers der Dienst *Windows Profile Server* gesetzt werden.

## Anmerkung

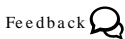
Für den reibungslosen Betrieb darf der Dienst nur an einem Dateiserver pro OU gesetzt werden. Weiterhin ist der Dienst *Windows Profile Server* veraltet und wird in einer zukünftigen UCS@school-Version entfernt bzw. durch einen äquivalenten Mechanismus ersetzt.

- Darüber hinaus wird auch automatisch der Pfad zum Heimatverzeichnis des Benutzers gesetzt. In einer Single-Server-Umgebung wird automatisch der Domaincontroller Master als Dateiserver eingetragen. In Multi-Server-Umgebungen ist der für die OU zuständige Dateiserver am OU-Objekt hinterlegt. Um diesen zu ändern, muss in der Univention Management Console das OU-Objekt geöffnet werden und auf dem Reiter *UCS@school* im Auswahlfeld *Server für Windows-Heimatverzeichnisse* ein geeigneter Dateiserver ausgewählt werden. Der dort definierte Dateiserver wird beim Anlegen eines Benutzers ausgelesen und der Pfad am Benutzerobjekt entsprechend gesetzt (Beispiel: `\\server3.example.com\benutzer123`).

## Anmerkung

Die Windows-spezifischen Einstellungen werden nur beim Anlegen eines Benutzers gesetzt. Ein nachträgliches Modifizieren des Benutzers über die Importskripte hat keinen Einfluss auf diese Einstellungen.

## 6.1.2. Manuelles Anlegen von Benutzerkonten für Mitarbeiter

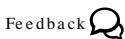


Benutzerkonten für Mitarbeiter können auch über das UMC-Modul **Benutzer** auf dem Domänencontroller Master angelegt werden.

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

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

## 6.1.3. Anlegen von Benutzerkonten für Schuladministratoren



Benutzerkonten von Lehrern können durch eine zusätzliche Gruppenmitgliedschaft zu Schuladministratoren umgewandelt werden. Sie unterliegen dann jedoch der Einschränkung, dass die Benutzerkonten der Lehrer-Schuladministratoren nur auf den edukativen Schulserver und nicht auf den Schulserver des Verwaltungsnetzes repliziert werden.

Die zusätzliche Gruppenmitgliedschaft muss manuell über das UMC-Modul **Benutzer** auf dem Domänencontroller Master hinzugefügt werden. Auf dem Reiter **Gruppen** muss das Benutzerkonto in die Gruppe *admins-OU* (bei der OU *gym17* ist dies die Gruppe *admins-gym17*) aufgenommen werden.

Soll das Benutzerkonten des Schuladministrators auch auf den Systemen des Verwaltungsnetzes verfügbar sein, so reicht es nicht aus, die Gruppenmitgliedschaft zu ändern. Es muss manuell ein neues Benutzerkonto über das UMC-Modul **Benutzer** auf dem Domänencontroller Master angelegt werden.

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

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

Sollte der Schuladministrator auch als Lehrer tätig sein, muss zusätzlich die Gruppe *lehrer-OU*, also z.B. *lehrer-gym17*, hinzugefügt werden.

Abschließend müssen die Angaben für Profilverzeichnispfad und Heimatverzeichnispfad am Benutzerobjekt gesetzt werden, um das gleiche Verhalten wie bei Schüler- und Lehrerkonten zu erhalten (siehe dazu auch Abschnitt 6.1.1).

## 6.2. Skriptgesteuerter Import von Klassen



Klassen 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 *IA* 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	---	g123m
Gruppenname	Der Name der Gruppe	---	g123m-1A
(Beschreibung)	Optionale Beschreibung der Gruppe	---	Klasse 1A

Ein Beispiel für eine Importdatei:

```
A g123m g123m-1A Klaaassen 1A
A g123m g123m-LK-Inf Leistungskurs Informatik
M g123m g123m-1A Klasse 1A
D g123m g123m-LK-Inf Leistungskurs Informatik
D g123m g123m-R12 Klasse R12
```

## 6.3. Vorgehen zum Schuljahreswechsel

Feedback 

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 Umbenennung 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

7.1. Anmeldedienste mit Samba .....	31
7.2. Server für Dateifreigaben .....	32
7.3. Netlogon-Skripte für Samba4-Umgebung .....	32
7.4. iTALC-Installation auf Windows-Clients .....	33

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.

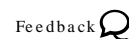
Die Netzkonfiguration der Clients kann zentral über in UCS integrierte DNS- und DHCP-Dienste durchgeführt werden. Weitere Hinweise finden sich in Abschnitt 5.4.2.

Beim Import von neuen Benutzern über die Importskripte oder über den Assistenten in der UMC werden automatisch windows-spezifische Einstellungen zum Profilverzeichnis und zum Heimatverzeichnis vorgenommen. Weitere Hinweise finden sich in Abschnitt 6.1.1.

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 7.4 beschrieben.

Aufgrund einiger Limitierungen (u.a. von iTALC) kann auf Windows-Terminalservern nicht der volle Funktionsumfang von UCS@school genutzt werden. Die Verwendung von Terminalservern mit UCS@school wird daher nicht unterstützt.

## 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 Multi-Server-Umgebung ist es zwingend erforderlich, dass alle Windows-Clients ihren jeweiligen Schul-DC als DNS-Server verwenden, um einen fehlerfreien Betrieb zu gewährleisten.



Windows-Clients, die ihre DNS-Einstellungen über DHCP beziehen, erhalten in der Standardeinstellung automatisch die IP-Adresse des Schul-DCs als DNS-Server zugewiesen. Dafür wird beim Joinen eines Schulservers automatisch am unter dem Schul-OU-Objekt liegenden DHCP-Container eine DHCP-DNS-Richtlinie verknüpft. Das automatische Verknüpfen dieser Richtlinie kann über das Setzen einer UCR-Variable auf dem Schulserver (bzw. dem Domänencontroller Master bei Single-Server-Umgebungen) deaktiviert werden. Die folgende Variable muss vor der Installation von UCS@school oder dem Update des Systems gesetzt werden:


```
ucr set ucsschool/import/generate/policy/dhcp/dns/
set_per_ou=false
```

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](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. Netlogon-Skripte für Samba4-Umgebung

Feedback 

In UCS-Umgebungen mit mehreren Samba4-Domänencontrollern werden in der Standardeinstellung alle Dateien der NETLOGON-Dateifreigabe automatisch (durch die SYSVOL-Replikation) zwischen allen Samba4-Domänencontrollern repliziert. Beim Einsatz von UCS@school kann es bei der Verwendung von domänenweiten Benutzerkonten und benutzerspezifischen Netlogon-Skripten zu Synchronisationskonflikten kommen. Konflikte können ebenfalls bei eigenen, standortbezogenen Netlogon-Skripten auftreten.

In diesen Fällen ist es ratsam, die Synchronisation der NETLOGON-Freigabe zu unterbinden, indem ein abweichendes Verzeichnis für die NETLOGON-Freigabe definiert wird. Das Verzeichnis darf dabei nicht unterhalb der SYSVOL-Dateifreigabe (`/var/lib/samba/sysvol/REALM/`) liegen.

Das folgende Beispiel setzt das Verzeichnis der NETLOGON-Freigabe auf `/var/lib/samba/netlogon/` und passt ebenfalls das Verzeichnis für die automatisch generierten Benutzer-NETLOGON-Skripte an:


```
ucr set samba/share/netlogon/path=/var/lib/samba/netlogon
ucr set ucsschool/userlogon/netlogon/path=/var/lib/samba/netlogon/user
```



Die zwei UCR-Variablen müssen auf allen Samba4-Domänencontrollern gesetzt werden. Dies kann z.B. in der UMC über eine UCR-Richtlinien global definiert werden. Nach der Änderung müssen die Dienste *samba4* und *univention-directory-listener* neu gestartet werden:

```
invoke-rc.d samba4 restart
invoke-rc.d univention-directory-listener restart
```

## 7.4. 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 die Software iTALC installiert wurde.

Seit UCS@school 3.1 R2 sind Windows-Binärpakete für die Open Source-Software iTALC in UCS@school enthalten. Die Binärpakete sind direkt über die Samba-Freigabe *iTALC-Installation* abruf- und installierbar. Alternativ finden sich die Installationsdateien für 32- und 64bit-Versionen von iTALC auf dem Schulserver im Verzeichnis `/usr/share/italc-windows/`. Interoperabilitätstests zwischen UCS@school und iTALC wurden ausschließlich mit der von UCS@school mitgelieferten iTALC-Version 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.

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). Der Dateiname der Schlüsseldatei enthält den Namen des Schulservers für den sie generiert wurde, um Namenskonflikte auf der SYSVOL-Freigabe bei der Verwendung von Samba 4

### *iTALC-Installation auf Windows-Clients*

zu vermeiden. Damit der iTALC-Assistent die Schlüsseldatei selbständig erkennt, sollte die Datei `italc-key_SERVERNAME.pub.key.txt` verwendet werden.

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 Konfigurationsparameter zusammengestellt. Die PAC-Datei eines Schulservers steht unter der folgenden URL bereit:

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

Im Internet Explorer 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

9.1. Installation und Konfiguration des RADIUS-Servers .....	37
9.2. Konfiguration der Access Points .....	37
9.3. Konfiguration der zugreifenden Clients .....	37
9.4. Freigabe des WLAN-Zugriffs in der Univention Management Console .....	38
9.5. Fehlersuche .....	38

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 Authentifizierungsmodus muss auf RADIUS-Authentifizierung 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 zunächst das UCS-Wurzelzertifikat importieren. Es kann z.B. von der Startseite des Domänencontroller Master unter dem Link "Wurzelzertifikat" bezogen werden. Anschließend muss er 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 Betriebssystem 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>, sowie für die Einrichtung unter Windows 7: <http://wiki.univention.de/index.php?title=Einrichtung-WLAN-Authentifizierung-Win7>.

## 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*.

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

10.1. Erweiterung von Importdateien .....	40
10.2. Beispiel-Hook-Skript: automatische Erstellung der Marktplatzfreigabe .....	40
10.3. Beispiel-Hook-Skript: Setzen des LDAP-Containers für DHCP-Objekte .....	41

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 Feedback

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.



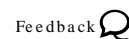
# Kapitel 11. Klassenarbeitsmodus

11.1. Technische Hintergründe .....	43
11.2. Konfiguration .....	44
11.3. Beispiele für Gruppenrichtlinien .....	45
11.3.1. Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen .....	46
11.3.2. Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken .....	46
11.3.2.1. Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken .....	46
11.3.2.2. Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer .....	47
11.3.3. Zugriff auf USB-Speicher und Wechselmedien einschränken .....	48
11.3.3.1. Zugriff auf USB-Speicher an Windows XP einschränken .....	48
11.3.3.2. Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten.....	48
11.3.3.3. Zugriff auf USB-Speicher an Windows 7 einschränken .....	49
11.3.3.4. Installation neuer Gerätetreiber für USB-Speicher an Windows 7 Clients verbieten .....	49
11.3.4. Vorgabe von Proxy-Einstellungen für den Internetzugriff .....	50
11.3.4.1. Proxy-Vorgabe für den Internet Explorer .....	50
11.3.4.2. Sperrung der Proxyeinstellung für den Internet Explorer .....	50
11.3.4.3. Proxy-Vorgabe für Google Chrome .....	50
11.3.4.4. Proxy-Vorgabe für Mozilla Firefox .....	51
11.3.5. Zugriff auf bestimmte Programme einschränken .....	52
11.3.5.1. Kommandoingabeaufforderung deaktivieren .....	52
11.3.5.2. Zugriff auf Windows-Registry-Editor deaktivieren .....	52
11.3.5.3. Konfiguration von Software Restriction Policies (SRP) .....	53

Der Klassenarbeitsmodus ermöglicht die gezielte Einschränkung der Computernutzung für Schüler einer Klasse. Über das UMC-Modul für den Klassenarbeitsmodus kann ein Lehrer einen Klassenraum für die exklusive Nutzung durch bestimmte Gruppen konfigurieren. Der Klassenarbeitsmodus bietet darüber hinaus auch einen direkten Zugriff auf die Funktionalitäten der Materialverteilung. Hintergründe zur technischen Umsetzung werden in Abschnitt 11.1 und mögliche Konfigurationsschnittstellen in Abschnitt 11.2 genannt.

Für die Dauer des Klassenarbeitsmodus werden die ausgewählten Schüler und Räume in eine speziell benannte Gruppe aufgenommen. Dies macht es möglich mit Hilfe von Windows-Gruppenrichtlinien spezifische Einschränkungen für die Benutzung von Windows-Rechnern im gewählten Raum zu definieren, wie z.B. die Vorgabe eines Proxy-Servers zur Filterung des Internetzugriffs, die Einschränkung den Zugriffs auf USB-Speicher und andere Wechselmedien oder auch die Sperrung bestimmter Programme. Einsatzmöglichkeiten für Gruppenrichtlinien werden in Abschnitt 11.3 beispielhaft beschrieben.

## 11.1. Technische Hintergründe



Zur Verwendung des Klassenarbeitsmodus sind folgende Voraussetzungen zu erfüllen:

- Verwendung einer Samba 4-Domäne (AD-Domäne)
- Einsatz von Windows XP oder höher auf den Prüfungscomputern
- Import von Computerkonten und Zuordnung der Computer zu Computerräumen
- Die Verwendung des UCS@school-HTTP-Proxys durch die Prüfungscomputer zur Filterung des Internetzugriffs

Eine neue Klassenarbeit kann über das Modul **Klassenarbeit starten** begonnen werden. Beim Durchlaufen der einzelnen Schritte werden von der Lehrkraft ein Name für die Klassenarbeit und die teilnehmenden Klassen/Arbeitsgruppen ausgewählt. Zusätzlich können für die Arbeit notwendige Dateien hochgeladen sowie Computerraumeinstellungen ausgewählt werden.

Damit Schülern nicht die Möglichkeit gegeben wird, auf ihr bisheriges Heimatverzeichnis zuzugreifen, werden zum Zeitpunkt des Einrichtens der Klassenarbeit für die ausgewählten Schülerkonten spezielle Klassenarbeitskonten neu angelegt. Der Loginname für das Klassenarbeitskonto setzt sich aus einem festgelegten Prefix (standardmäßig *exam-*) und dem normalen Benutzernamen zusammen. Bspw. wird für den Benutzer *anton123* das Klassenarbeitskonto *exam-anton123* angelegt, mit dem er sich während der Klassenarbeit anmelden muss. Für das Klassenarbeitskonto wird ein neues Heimatverzeichnis erzeugt, Passwörter und andere Konteneinstellungen werden jedoch aus dem ursprünglichen Benutzerkonto direkt übernommen.

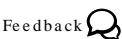
Alle Klassenarbeitskonten der Schüler sowie alle Rechner des Computerraumes sind für den Zeitraum der Klassenarbeit Mitglieder der Gruppe *OU<OU-Name>-Klassenarbeit*. Durch diese Gruppe können spezifische Einschränkungen für Schüler und Rechner mit Hilfe von Windows-Gruppenrichtlinien vorgenommen werden (siehe Abschnitt 11.3).

### Anmerkung

Damit die Einstellungen der Gruppenrichtlinien für die Rechner entsprechend greifen, ist es wichtig, dass die Schülerrechner des Computerraumes nach dem Einrichten einer Klassenarbeit neu gestartet werden. Dieser Vorgang wird durch das UMC-Modul **Klassenarbeit starten** unterstützt, indem alle eingeschalteten Rechner automatisch neu gestartet werden können. Zusätzlich ist es aus dem selben Grund wichtig, dass nach Beenden einer Klassenarbeit die Schülerrechner entweder ausgeschaltet oder neu gestartet werden. Nur so können die ursprünglichen Einstellungen der Gruppenrichtlinien wieder wirksam werden.

Damit leicht erkannt werden kann, dass die Gruppenrichtlinien für den Klassenarbeitsmodus an den Rechnern wirksam sind, empfehlen wir, bspw. ein optisch klar zu unterscheidendes Hintergrundbild über die Richtlinien zuzuweisen.

## 11.2. Konfiguration



Für die Konfiguration des Klassenarbeitsmodus gibt es eine Reihe von Univention Configuration Registry-Variablen. Diese werden im folgenden aufgelistet und kurz erläutert.


Die nachfolgenden Univention Configuration Registry-Variablen können geändert werden, um LDAP-Eigenschaften der Klassenarbeitskonten, -gruppen und -container anzupassen. Sofern diese Variablen manuell gesetzt werden, ist zu beachten, dass es sich dabei um globale Einstellungen handelt und diese Variablen sowohl auf dem Domänencontroller Master als auch auf den Schulservern identische Werte aufweisen müssen.

- `ucsschool/ldap/default/userprefix/exam` gibt den Prefix an, der dem ursprünglichen Benutzernamen im Klassenarbeitskonto vorangestellt wird. Er ist standardmäßig auf *exam-* gesetzt.
- `ucsschool/ldap/default/groupname/exam` bezeichnet die Gruppe, der alle Klassenarbeitskonten sowie Klassenarbeitsrechner zugeordnet sind. Über diese Gruppe können spezifische Windows-Gruppenrichtlinien für den Klassenarbeitsmodus gesetzt werden. Der Standardname für diese Gruppe ist *OU %(ou)s-Klassenarbeit*, wobei *%(ou)s* vom System automatisch durch den Namen der OU ausgetauscht wird.
- `ucsschool/ldap/default/container/exam` ist der Name des Containers, unterhalb dem die Klassenarbeitskonten gespeichert werden. Standardmäßig ist der Name auf *examusers* gesetzt. Die LDAP-Position des Containers ist direkt unterhalb der Schul-OU.

Das UMC-Modul zum Einrichten einer Klassenarbeit bietet die Möglichkeit bestimmte Standardwerte zu definieren, um das Starten einer Klassenarbeit zu vereinfachen; dazu gehören:

- `ucsschool/exam/default/room` definiert den vorausgewählten Raum für eine neue Klassenarbeit. Der Eintrag beinhaltet den LDAP-Namen des Raumes (inklusive des Schul-OU-Präfixes), also bspw. *meineschule-PC Raum*. Ist die Variable nicht gesetzt, wird standardmäßig der alphabetisch erste Raum ausgewählt.
- `ucsschool/exam/default/shares` gibt den vorausgewählten Freigabezugriff für eine neue Klassenarbeit an. Mögliche Werte sind *all* für Zugriff auf alle Freigaben ohne Einschränkungen sowie *home* für eingeschränkten Zugriff auf lediglich das Heimatverzeichnis des (Klassenarbeits-)Benutzerkonto. Ist die Variable nicht gesetzt, wird standardmäßig nur der Zugriff auf das Homeverzeichnis freigegeben.
- `ucsschool/exam/default/internet` definiert die vorausgewählte Internetregel für eine neue Klassenarbeit. Mögliche Werte umfassen die Namen aller Internetregeln wie sie im UMC-Modul **Internetregeln definieren** angezeigt werden. Normalerweise werden die globalen Standardeinstellungen verwendet.

## 11.3. Beispiele für Gruppenrichtlinien

Feedback 

Gruppenrichtlinien werden von einem Windows System aus mit Hilfe der Gruppenrichtlinienverwaltung (GPMC) angelegt und bearbeitet. Im Folgenden ist die Konfiguration der Gruppenrichtlinien von einem Windows 7 System aus beschrieben auf dem dazu die Gruppenrichtlinienverwaltung (GPMC) aus den Remote System Administration Tools (RSAT) installiert sein muss.

Alle Gruppenrichtlinieneinstellungen können je nach Bedarf gesammelt über ein Gruppenrichtlinienobjekt vorgenommen werden oder auf separate Objekte verteilt werden. Um den Bezug zwischen einem ausgewählten Gruppenrichtlinienobjekt und Objekten im Samba-Verzeichnisdienst herzustellen, kann es mit einer Organisationseinheit (OU) verknüpft werden, z.B. der Schul-OU. Einige der hier beispielhaft beschriebenen Gruppenrichtlinieneinstellungen wirken sich nur auf Benutzer- und andere nur auf Computer-Konten aus. Da die Einstellungen eines Gruppenrichtlinienobjekts nur für Objekte ausgewertet werden, die unterhalb des speziellen Verzeichniszweigs liegen, mit dem es verknüpft wurde, ist es wichtig, dass das entsprechende Gruppenrichtlinienobjekt hinreichend hoch in der hierarchischen Objektordnung verknüpft wird.

Einige der genannten Gruppenrichtlinien-Einstellungen beziehen sich auf den Bereich der Computerkonfiguration und werden nur beim Systemstart korrekt von den entsprechenden Windows-Komponenten ausgewertet. Für solche Einstellungen ist daher ein Neustart der Windows-Arbeitsplatzsysteme nach Aktivierung des Klassenarbeitsmodus notwendig.

### Anmerkung

Zu diesem Thema ist auch ein Hinweis von Microsoft zu Windows XP Systemen zu beachten: „Jede Version von Windows XP Professional stellt eine Funktion zur Optimierung für schnelles Anmelden zur Verfügung. Computer mit diesen Betriebssystemen warten standardmäßig beim Starten nicht auf den Start des Netzwerks. Nach der Anmeldung werden die Richtlinien im Hintergrund verarbeitet, sobald das Netzwerk zur Verfügung steht. Dies bedeutet, dass der Computer bei der Anmeldung und beim Start weiterhin die älteren Richtlinieneinstellungen verwendet. Daher sind für Einstellungen, die nur beim Start oder bei der Anmeldung angewendet werden können (z. B. Softwareinstallation und Ordnerumleitung), möglicherweise nach dem Ausführen der ersten Änderung am Gruppenrichtlinienobjekt mehrere Anmeldungen durch den Benutzer erforderlich. Diese Richtlinie wird gesteuert durch die Einstellung in `Computerkonfiguration\Administrative Vorlagen\System\Anmeldung\Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten`. Diese Funktion ist in den Betriebssystemversionen von Windows 2000 oder Windows Server 2003 nicht verfügbar.“<sup>1</sup>

<sup>1</sup>[http://technet.microsoft.com/de-de/library/cc785665\(v=ws.10\).aspx](http://technet.microsoft.com/de-de/library/cc785665(v=ws.10).aspx)

## 11.3.1. Generelle Hinweise zu Gruppenrichtlinien und Administrativen Vorlagen Feedback

Auf dem Schulserver sollte das Verzeichnis `/var/lib/samba/sysvol/DomänenNameDerUCS@schoolUmgebung/Policies/PolicyDefinitions/` angelegt werden. Sobald dieses Verzeichnis angelegt ist, bevorzugt das Windows-Programm zur Gruppenrichtlinienverwaltung die dort hinterlegten Administrativen Vorlagen im ADMX-Format vor den lokal auf dem Windows 7 System installierten Administrativen Vorlagen.

Da in den nachfolgenden Abschnitten zusätzliche Administrative Vorlagen verwendet werden, die ebenfalls in dem oben genannten Verzeichnis abzulegen sind, wird empfohlen, nach dem Erstellen des Verzeichnisses einmalig die lokal installierten Administrativen Vorlagen aus dem Verzeichnis `C:\Windows\PolicyDefinitions` in das neue Verzeichnis zu kopieren. Da das Verzeichnis serverseitig unterhalb der SYSVOL-Freigabe liegt, wird es per Voreinstellung auf alle Samba 4-Server der Domäne synchronisiert. Die Administrativen Vorlagen sind an sich keine Gruppenrichtlinien, sie dienen nur zur Erweiterung der Einstellungsmöglichkeiten die das Windows Programm zur Gruppenrichtlinienverwaltung dem Administrator zur Auswahl anbietet. Für neuere Windows-Versionen, wie z.B. Windows 8 stellt Microsoft aktualisierte Administrative Vorlagen zum Download zur Verfügung.

Grundsätzlich können Gruppenrichtlinien im Samba-Verzeichnisdienst mit Organisationseinheiten (OU) und der LDAP-Basis verknüpft werden. Im UCS@school-Kontext werden jedoch nur Verknüpfungen unterhalb der Schul-OU auch automatisch in das OpenLDAP-Verzeichnis synchronisiert. Verknüpfungen mit der LDAP-Basis werden z.B. durch OpenLDAP-Zugriffsbeschränkungen blockiert, damit sich eine Anpassung der damit verknüpften Gruppenrichtlinien durch einen Schul-Administrator nicht auch auf alle anderen Schulen auswirkt. Eine solche Änderung wird im S4-Connector auf der Schule als Reject notiert. Wenn tatsächlich gewünscht ist, eine Änderung der Gruppenrichtlinienverknüpfung an der LDAP-Basis und unter `OU=Domain Controllers` auch in das OpenLDAP-Verzeichnis und damit an alle Schulen zu synchronisieren, kann auf dem Schulserver folgender Befehl mit dem zentralen Administrator-Passwort ausgeführt werden:

```
eval "$(ucr shell)"
/usr/share/univention-s4-connector/msgpo.py --write2ucs \
  --binddn "uid=Administrator,cn=users,$ldap_base" --bindpwd <password>
```

Der S4-Connector erkennt eine kurze Zeit später bei dem nächsten Resync, dass der Reject aufgelöst wurde.

## 11.3.2. Windows-Anmeldung im Prüfungsraum auf Mitglieder der Klassenarbeitsgruppe beschränken Feedback

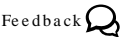
Da das im folgenden konfigurierte Gruppenrichtlinienobjekt je nach Verknüpfung im Samba-Verzeichnisdienst die Anmeldung an betroffenen Windows-Arbeitsplatzsystemen einschränkt, wird dringend empfohlen, als erstes die Anwendung der neuen Gruppenrichtlinie auf solche Windows-Arbeitsplatzsysteme einzuschränken, auf die sie sich später im Klassenarbeitsmodus auswirken soll. Dies geschieht am einfachsten über die Anpassung der Sicherheitsfilterung, die im Folgenden beschrieben ist:

### 11.3.2.1. Anwendungsbereich der GPO auf Klassenarbeitscomputer einschränken Feedback

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- In der Baumdarstellung der Gruppenrichtlinienverwaltung die Gruppenrichtlinie anklicken.
- Auf dem geöffneten Reiter *Bereich* im Abschnitt *Sicherheitsfilterung* die Schaltfläche *Hinzufügen* betätigen.

- In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen der Klassenarbeitsgruppe (OUNameDerOU-Klassenarbeit, z.B. OUgym17-Klassenarbeit) eintragen und den Dialog mit *OK* schließen.
- Auf dem geöffneten Reiter *Bereich* im Abschnitt *Sicherheitsfilterung* die Gruppe *Authenticated Users* auswählen und die Schaltfläche *Entfernen* betätigen.

### 11.3.2.2. Einschränkung der Windows-Anmeldung auf Klassenarbeitsbenutzerkonten und Lehrer



- In der Gruppenrichtlinienverwaltung das Gruppenrichtlinienobjekt zur Bearbeitung öffnen (Kontextmenü des GPO in der Baumdarstellung).
- Im neu geöffneten Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  
`Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten`
- Im neu geöffneten Richtlinien-Dialog *Eigenschaften von Lokal anmelden zulassen* auf dem Reiter *Sicherheitsrichtlinie* die Option *Diese Richtlinieneinstellung definieren* aktivieren.
- Dann die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
- Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
- In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen *Administratoren* eintragen und den Dialog mit *OK* schließen.
- Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
- Erneut die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
- Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
- In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen der Klassenarbeitsgruppe (OUNameDerOU-Klassenarbeit, z.B. OUgym17-Klassenarbeit) eintragen und den Dialog mit *OK* schließen.
- Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
- Erneut die Schaltfläche *Benutzer oder Gruppe hinzufügen* betätigen.
- Im neu geöffneten Dialog die Schaltfläche *Durchsuchen* betätigen.
- In das Eingabefeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen der Lehrergruppe (Lehrer-NameDerOU, z.B. lehrer-gym17) eintragen und den Dialog mit *OK* schließen.
- Den Dialog *Benutzer oder Gruppe hinzufügen* ebenfalls mit *OK* schließen.
- Den Richtlinien-Dialog *Eigenschaften von Lokal anmelden zulassen* mit *OK* schließen.

Damit die Gruppenrichtlinieneinstellungen von Windows-Arbeitsplatzrechnern ausgewertet werden, ist es notwendig, einen Bezug zwischen dem angelegten Gruppenrichtlinienobjekt und den Rechnerobjekten im Samba-Verzeichnisdienst herzustellen. Um dies zu erreichen kann das Gruppenrichtlinienobjekt mit einer Organisationseinheit (OU) verknüpft werden, die den Rechnerobjekten im Verzeichnisbaum übergeordnet ist, in der Regel mit der Schul-OU.



### 11.3.3. Zugriff auf USB-Speicher und Wechselmedien einschränken Feedback

Zur Einschränkung des Zugriffs auf USB-Speicher und Wechselmedien sind je nach Windowsversion zwei Fälle zu beachten: einerseits die Einschränkung der Benutzung bereits installierter Gerätetreiber und andererseits die Einschränkung der Installation neuer Gerätetreiber.

Während für Windows XP beide Einschränkungen notwendig sind, bietet Windows 7 durch erweiterte Richtlinien vereinfachte und erweiterte Kontrollmöglichkeiten. In Mischumgebungen ist eine Kombination der skizzierten Einstellungen zu empfehlen.

#### Anmerkung

Die Liste der hier erwähnten Einstellungen erhebt nicht den Anspruch auf Vollständigkeit. Es ist notwendig die Einstellungen entsprechend der lokalen Gegebenheiten zu testen. Insbesondere sollte folgende Microsoft-Dokumentation beachtet werden:

- <http://technet.microsoft.com/de-de/library/hh125922%28v=ws.10%29.aspx>.

#### 11.3.3.1. Zugriff auf USB-Speicher an Windows XP einschränken Feedback

Diese Richtlinie wird über eine Administrative Vorlage (ADMX) definiert, die in Microsoft Knowledgebase Artikel 555324.<sup>2</sup> beschrieben ist. Erst nach Einbinden der Administrative Vorlage (ADMX) können folgende Einstellungen getroffen werden. Beispiele für ADMX-Dateien liegen unter `/usr/share/doc/ucs-school-umc-exam/examples/GPO`. Zum Einbinden der ADMX-Dateien müssen diese auf die `SYSVOL`-Freigabe kopiert werden (siehe Abschnitt 11.3.1).

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

Computerkonfiguration > Richtlinien > Administrative Vorlagen > Spezielle Einstellungen > Treiber einschränken

- Richtlinie *USB Sperren* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

#### Anmerkung

Hier stehen auch weitere Gerätetypen zur Auswahl, z.B. CD-ROM-Laufwerke.

#### 11.3.3.2. Installation neuer Gerätetreiber für USB-Speicher an Windows XP verbieten Feedback

Diese Richtlinie definiert eingeschränkte Dateisystemberechtigungen gemäß Microsoft Knowledgebase Artikel 823732<sup>3</sup>.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Dateisystem

- Rechtsklick auf *Datei hinzufügen...*


<sup>2</sup><http://support.microsoft.com/kb/555324>

<sup>3</sup><http://support.microsoft.com/kb/823732>



- Das Verzeichnis `C:\Windows\Inf` ansteuern und dort die Datei `usbstor.inf` auswählen und mit *OK* bestätigen (ggf. wird die Dateiendung `.inf` nicht mit angezeigt).
- In dem neu geöffneten Dialog *Datenbanksicherheit für ...* in der oberen Liste *Gruppen- oder Benutzernamen* die Schaltfläche *Hinzufügen* betätigen und den Namen der Klassenarbeitsgruppe hinzufügen,
- In der darunter angezeigten Liste *Berechtigungen für ...* in der Zeile *Vollzugriff*, Spalte *Verweigern* ein Häkchen setzen und mit *OK* bestätigen.
- Den Dialog *Datenbanksicherheit für ...* mit *OK* schließen.
- Das neue Dialogfenster *Windows-Sicherheit* mit *Ja* bestätigen.
- Das neue Dialogfenster *Objekt hinzufügen* mit *OK* schließen.
- Analog sollten Einstellungen für `%SystemRoot%\inf\usbstor.pnf` und `%SystemRoot%\system32\drivers\usbstor.sys` definiert werden.

### 11.3.3.3. Zugriff auf USB-Speicher an Windows 7 einschränken


Feedback 

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  
`Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > System > Wechselmedienzugriff`
- Z.B. Richtlinie *Wechseldatenträger: Lesezugriff verweigern* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.

#### **Anmerkung**

Weitere Informationen zu diesem Thema liefert z.B. <http://technet.microsoft.com/de-de/library/cc771759%28v=ws.10%29.aspx>.

### 11.3.3.4. Installation neuer Gerätetreiber für USB-Speicher an Windows 7 Clients verbieten

Feedback 

Zusätzliche Einschränkungen zur Installation von Gerätetreibern sind auch unter Windows 7 möglich. Die Einstellungsmöglichkeiten bieten eine größere Kontrolle, setzen aber auch konkrete Erfahrungen mit den im Einzelfall eingesetzten Geräten voraus. Daher ist dieser Abschnitt nur als Einstiegshilfe zu verstehen. Die folgende Einstellung würde die zusätzliche Installation jeglicher Treiber für Wechselgeräte deaktivieren. Es kann hier z.B. dann zusätzlich sinnvoll sein, Administratoren von dieser Einschränkung auszunehmen.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  
`Computerkonfiguration > Richtlinien > Administrative Vorlagen > System > Geräteinstallation > Einschränkungen bei der Geräteinstallation`
- Hier kann die Installation von Treibern für bestimmte Geräteklassen, Geräte-IDs oder alle Wechselgeräte eingeschränkt werden.
- Richtlinie *Installation von Wechselgeräten verhindern* öffnen, *Aktiviert* auswählen und mit *OK* bestätigen.


## Vorgabe von Proxy-Einstellungen für den Internetzugriff

- Die Richtlinie *Administratoren das Außerkraftsetzen der Richtlinien unter ... erlauben* erlaubt Mitgliedern der Administratorengruppe die getroffenen Einschränkungen zu umgehen.
- Noch stärkere Restriktionen sind möglich, indem man die Ausschlusslogik auf Whitelisting umstellt. Dies kann über die Richtlinie *Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind* erreicht werden.

### Anmerkung

Weitere Informationen zu diesem Thema liefert z.B. <http://technet.microsoft.com/de-de/library/cc731387%28v=ws.10%29.aspx>.


## 11.3.4. Vorgabe von Proxy-Einstellungen für den Internetzugriff

Feedback 

Im Folgenden sind Vorgaben für Internet Explorer, Google Chrome und Mozilla Firefox beschrieben. Während Microsoft selbst Administrative Vorlagen mitliefert, sind für Google Chrome und Mozilla Firefox jeweils eigene Administrative Vorlagen notwendig.

Zusätzlich zur Vorgabe einer Proxyeinstellung ist für den Klassenarbeitsmodus eine Sperrung des Benutzer-Zugriffs auf eben diese Einstellungen sinnvoll. Dazu gibt es zwei unterschiedliche Ansätze: Im Fall des Internet Explorers bietet die Administrative Vorlage die Möglichkeit, das entsprechende Einstellungsfenster zu sperren. Im Fall von Google Chrome und Mozilla Firefox werden hingegen die Proxy-Einstellungen per Gruppenrichtlinie für den Arbeitsplatzrechner vorgegeben, statt für den Benutzer, und sind dadurch z.B. für Schüler nicht mehr veränderbar. Für die beiden letztgenannten Browser ist es daher wichtig darauf zu achten, die Einstellungen, wo nötig, im Zweig *Computerkonfiguration* des Gruppenrichtlinieneditors statt im Zweig *Benutzerkonfiguration* zu treffen.

### 11.3.4.1. Proxy-Vorgabe für den Internet Explorer


Feedback 

- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

Benutzerkonfiguration > Richtlinien > Windows-Einstellungen > Internet Explorer-Wartung > Verbindung

- Richtlinie *Proxyeinstellungen* öffnen, *Aktiviert* auswählen und bestätigen.
- Proxyadresse für *HTTP* sowie *Secure* und das entsprechende *Port*-Feld ausfüllen (Wert der Univention Configuration Registry-Variable `squid/httpport`, Standard 3128)
- Ggf. *Für alle Adressen denselben Proxyserver verwenden* aktivieren.

### 11.3.4.2. Sperrung der Proxyeinstellung für den Internet Explorer


Feedback 

- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

Computerkonfiguration > Richtlinien > Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien) > Windows-Komponenten > Internet Explorer > Internetsystemsteuerung

- Richtlinie *Verbindungsseite deaktivieren* öffnen und *Aktiviert* auswählen und bestätigen.

### 11.3.4.3. Proxy-Vorgabe für Google Chrome

Feedback 


Die Administrativen Vorlagen für Google Chrome werden durch das Zip-Archiv `policy_templates.zip` des Chromium-Projekts bereitgestellt. Die entsprechenden Dateien liegen unter `/usr/share/doc/ucs-school-umc-exam/examples/GPO`. Der Inhalt des `admx`-Verzeichnisses sollte in das Verzeichnis `PolicyDefinitions` auf den Schulserver kopiert werden, so dass dort die Datei

chrome.admx liegt. Die \*.adml-Dateien aus den Unterverzeichnissen müssen in gleichnamige Unterverzeichnisse unter PolicyDefinitions kopiert werden.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  

```
Computerkonfiguration > Richtlinien > Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien) > Google > Google Chrome > Proxy-Server
```
- Richtlinie *Auswählen, wie Proxy-Server-Einstellungen angegeben werden* öffnen und *Aktiviert* auswählen,
- Im Dropdown *System-Proxy-Einstellungen verwenden* auswählen und bestätigen.

#### 11.3.4.4. Proxy-Vorgabe für Mozilla Firefox

Feedback 

Auf dem Schulserver sollte das Verzeichnis `/var/lib/samba/sysvol/DomänenNameDerUCS@schoolUmgebung/Policies/PolicyDefinitions/` angelegt werden. Nähere Informationen sind im Abschnitt zu Google Chrome zu finden.

Die Administrativen Vorlagen für Mozilla Firefox werden durch das FirefoxADM-Projekt bereitgestellt. Es ist sinnvoll die dort definierten ADM-Vorlagen in das ADMX-Format umzuwandeln. Beispiele für ADMX Dateien liegen unter `/usr/share/doc/ucs-school-umc-exam/examples/GPO`. Der Inhalt des admx-Verzeichnisses sollte in das Verzeichnis PolicyDefinitions auf den Schulserver kopiert werden, so dass dort die Datei `firefoxlock.admx` liegt. Die \*.adml-Dateien aus den Unterverzeichnissen müssen in gleichnamige Unterverzeichnisse unter PolicyDefinitions kopiert werden.

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  

```
Computerkonfiguration > Richtlinien > Administrative Vorlagen: Vom zentralen Computer abgerufene Richtliniendefinitionen (ADMX-Dateien) > Mozilla Firefox Locked Settings > General
```
- Richtlinie *Proxy Settings* öffnen und *Aktiviert* auswählen,
- Im Dropdown *Preference State* die Einstellung *Locked* auswählen,
- Im Dropdown *Proxy Setting* die Einstellung *Manual Proxy Configuration* auswählen,
- Im Feld *Proxy Setting* die Einstellung *Manual Setting - HTTP Proxy* eintragen,
- Im Feld *HTTP Proxy Port* den Proxy Port eintragen (Wert der Univention Configuration Registry-Variable `squid/httpport`, Standard 3128)
- Den Dialog mit *OK* bestätigen.

Da Mozilla Firefox bisher nicht selbständig die über die Administrativen Vorlagen definierten Einstellungen in der Windows-Registry berücksichtigt, ist es notwendig diese Einstellungen über ein Startup- bzw. Shutdown-Skript in Mozilla-Konfigurationsdateien übersetzen zu lassen. Das FirefoxADM-Projekt stellt diese Skripte in Form von zwei vbs-Dateien zur Verfügung. Deren Einbindung ist über die folgenden Schritt möglich.


- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:

## Zugriff auf bestimmte Programme einschränken

Computerkonfiguration > Windows-Einstellungen > Skripts (Start/Herunterfahren)

- Richtlinie *Starten* öffnen,
- Im Dialog *Eigenschaften von Starten* auf dem Reiter *Skripts* die Schaltfläche *Dateien anzeigen* betätigen,
- In das vom automatisch geöffneten Windows Explorer angezeigte (leere) Verzeichnis (Machinese\Scripts\Startup im betreffenden GPO-Verzeichnis) die Datei `firefox_startup.vbs` kopieren und das Explorer-Fenster schließen.
- Im Dialog *Eigenschaften von Starten* die Schaltfläche *Hinzufügen* betätigen,
- Im neu geöffneten Dialog *Hinzufügen eines Skripts* neben dem Feld *Skriptname* den Namen `firefox_startup.vbs` eintragen und Dialog mit *OK* bestätigen.
- Im Dialog *Eigenschaften von Starten* den Dialog mit *OK* bestätigen.
- Richtlinie *Herunterfahren* öffnen, und dort analog zu dem Vorgehen bei *Starten* das Skript `firefox_shutdown.vbs` eintragen. Im Detail also:
- Im Dialog *Eigenschaften von Herunterfahren* die Schaltfläche *Hinzufügen* betätigen,
- In das vom automatisch geöffneten Windows Explorer angezeigte (leere) Verzeichnis (Machinese\Scripts\Shutdown im betreffenden GPO-Verzeichnis) die Datei `firefox_shutdown.vbs` kopieren und das Explorer-Fenster schließen.
- Im neu geöffneten Dialog *Hinzufügen eines Skripts* neben dem Feld *Skriptname* den Namen `firefox_shutdown.vbs` eintragen und Dialog mit *OK* bestätigen.
- Im Dialog *Eigenschaften von Herunterfahren* den Dialog mit *OK* bestätigen.

### 11.3.5. Zugriff auf bestimmte Programme einschränken


 Feedback 

#### Anmerkung

Die Liste der hier erwähnten Einstellungen erhebt nicht den Anspruch der Vollständigkeit. Es ist notwendig die Einstellungen entsprechend der lokalen Gegebenheiten zu testen. Insbesondere sollten folgende Microsoft-Dokumentationen beachtet werden:


- <http://technet.microsoft.com/en-us/library/bb457006.aspx#EGAA>.
- <http://technet.microsoft.com/en-us/library/hh994606.aspx>.

#### 11.3.5.1. Kommandozeile deaktivieren

 Feedback 

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  
 Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > System
- Richtlinie *Zugriff auf Eingabeaufforderung verhindern* öffnen und *Aktiviert* auswählen und bestätigen.

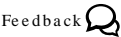
#### 11.3.5.2. Zugriff auf Windows-Registry-Editor deaktivieren

 Feedback 

- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.

- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  
Benutzerkonfiguration > Richtlinien > Administrative Vorlagen > System
- Richtlinie *Zugriff auf Programme zum Bearbeiten der Registrierung verhindern* öffnen
- *Aktiviert* auswählen und den Dialog mit *OK* bestätigen.

### 11.3.5.3. Konfiguration von Software Restriction Policies (SRP)



Aufgrund der Tiefe des Eingriffs der Software Restriction Policies ist zu empfehlen, diese zunächst in einer Testumgebung zu ausprobieren. Bei der Analyse von Zugriffsfehlern kann die Ereignisanzeige des Windows-Clients helfen <sup>4</sup>.

Die Software Restriction Policies greifen auch in die Bearbeitung von Login- und Logoff-Skripten ein. Alle dort verwendeten Programme bzw. Programmpfade sollten auf Ausführbarkeit getestet werden.

#### Anmerkung

Die Liste der hier erwähnten Einstellungen erhebt nicht den Anspruch der Vollständigkeit. Es ist notwendig die Einstellungen entsprechend der lokalen Gegebenheiten zu testen. Insbesondere sollte folgende Microsoft-Dokumentation beachtet werden:

- <http://technet.microsoft.com/en-us/library/bb457006.aspx#EGAA>.
- <http://technet.microsoft.com/en-us/library/hh994606.aspx>.
- In der Gruppenrichtlinienverwaltung ein neues Gruppenrichtlinienobjekt anlegen und/oder ein existierendes Gruppenrichtlinienobjekt zur Bearbeitung öffnen.
- Im Gruppenrichtlinienverwaltungseditor den folgenden Zweig öffnen:  
Benutzerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für Softwareeinschränkung
- Rechtsklick auf *Neue Richtlinien für Softwareeinschränkung erstellen*
- Im rechten Fensterteil *Erzwingen* öffnen,
- Einstellung *Alle Benutzer außer den lokalen Administratoren* auswählen und mit *OK* bestätigen.
- Im rechten Fensterteil *Sicherheitsstufen* öffnen.
- *Nicht erlaubt* per Doppelklick öffnen.
- *Als Standard* auswählen und mit *OK* bestätigen.
- Im rechten Fensterteil *Zusätzliche Regeln* öffnen.
- Rechtsklick auf *Neue Pfadregel...*
- In das Eingabefeld *Pfad* den UNC-Pfad `\\%USERDNSDOMAIN%\SysVol` eingeben, damit Logon- und GPO-Skripte ausgeführt werden können.
- In der Dropdown-Liste *Nicht eingeschränkt* auswählen und mit *OK* bestätigen.

<sup>4</sup> Weitere sinnvolle Hinweise zur Analyse und Pflege der Software Restriction Policies liefert z.B. [http://www.nsa.gov/ia/\\_files/os/win2k/Application\\_Whitelisting\\_Using\\_SRP.pdf](http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf)

**Tabelle 11.1. Beispiele für weitere Pfadregeln**

Pfad	Sicherheitsstufe
\\%USERDNSDOMAIN%\SysVol	Nicht eingeschränkt
\\%LogonServer%\SysVol	Nicht eingeschränkt
\\%LogonServer%\netlogon	Nicht eingeschränkt
\\%COMPUTERNAME%\Templates\*	Nicht eingeschränkt
%UserProfile%\Local Settings\Temp\*.tmp	Nicht eingeschränkt
%WinDir%\system32\cscript.exe	Nicht eingeschränkt
%WinDir%\system32\wscript.exe	Nicht eingeschränkt
%ProgramFiles%	Nicht eingeschränkt
%ProgramFiles(x86)%	Nicht eingeschränkt
*.lnk	Nicht eingeschränkt

- Es kann sinnvoll sein zusätzlich Programm-Pfade als *Nicht erlaubt* einzustufen, z.B.:

**Tabelle 11.2. Beispiele für weitere Pfadregeln**

Pfad	Sicherheitsstufe
%UserProfile%\Local Settings\Temp	Nicht erlaubt
%SystemRoot%\temp\*	Nicht erlaubt
%SystemRoot%\System32\mstsc.exe	Nicht erlaubt
%SystemRoot%\System32\dllcache\*	Nicht erlaubt
%SystemRoot%\System32\command.com	Nicht erlaubt
%SystemRoot%\System32\cmd.exe	Nicht erlaubt
%SystemRoot%\repair\*	Nicht erlaubt
%SystemDrive%\temp\*	Nicht erlaubt

- Es sollte beachtet werden, dass schreibbare Verzeichnisse, auf die der Zugriff nicht per Software Restriction Policy eingeschränkt ist, Benutzern die Möglichkeit geben, Programmdateien dort abzulegen und so die definierten Regeln zu umgehen<sup>5</sup>.

<sup>5</sup> Weitere sinnvolle Hinweise zur Analyse und Pflege der Software Restriction Policies liefert z.B. [http://www.nsa.gov/ia/\\_files/os/win2k/Application\\_Whitelisting\\_Using\\_SRP.pdf](http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf)

# Kapitel 12. Integration und Verwaltung von Univention Corporate Client-Systemen

12.1. Installation von UCC .....	56
12.2. Konfigurationseinstellungen für UCC-Systeme .....	56
12.3. Ausrollen von neuen UCC-Systemen .....	57

Univention Corporate Client (UCC) ist wie UCS@school eine aus dem Univention App Center heraus installierbare Erweiterung für Univention Corporate Server. UCC enthält eine optimierte Desktop-Umgebung auf Basis von Linux (Ubuntu), die eine Anpassung des Desktops an die jeweilige Hardware und den Einsatzzweck zulässt. Der Rollout der UCC-Systeme wird über ein imagebasiertes Verfahren durchgeführt. Dabei kann entweder auf offiziell bereitgestellte Images (ThinClient oder Desktop) zurückgegriffen werden oder es können speziell an die eigene Umgebung angepasste Images erstellt werden. Die Verwaltung der UCC-Systeme erfolgt über die Univention Management Console.

UCS@school bietet die Möglichkeit, UCC-Desktop-Systeme ähnlich wie Windows-Systeme in die UCS@school-Umgebung einzubinden. Die dafür notwendigen Konfigurationsschritte werden durch spezielle Integrationspakete für UCS@school und UCC auf ein Minimum reduziert. Nach dem Einbinden der UCC-Systeme stehen in Verbindung mit UCS@school unter anderem die folgenden Features auf den UCC-Systemen zur Verfügung:

- Automatisches Einbinden der Heimatverzeichnisse der Benutzer während des Anmeldevorgangs und der Zugriff auf Klassen- und Arbeitsgruppen-Dateifreigaben über eine Verknüpfung auf dem Desktop
- Automatische Einbindung der CUPS-Druckerfreigaben vom Schulserver
- Automatischer Start von iTALC auf den UCC-Systemen, welches die Verwendung der Bildschirm- bzw. Eingabegerätesperre über das UMC-Modul *Computerraum* ermöglicht
- Über Univention Configuration Registry-Richtlinien gesteuerte Einrichtung des Proxy-Servers für KDE-Anwendungen und Firefox inklusive einer transparenten Authentifizierung gegenüber dem HTTP-Proxy (Squid) des Schulservers


Für die Integration von UCC in UCS@school gelten die folgenden Einschränkungen:

- Für die Integration von UCC-Desktop-Systemen in UCS@school ist die Verwendung von Samba 4 auf dem UCS@school-Schulserver erforderlich.
- Die UCC-Systeme müssen mit dem offiziellen Desktop-Image (oder einem äquivalenten, selbsterstellten Image) installiert werden. UCC-ThinClient-Systeme bzw. UCC-Terminalserver werden in Verbindung mit UCS@school nicht unterstützt.
- Der über iTALC realisierte Präsentationsmodus sowie das Beaufsichtigen von Systemen über das UMC-Modul *Computerraum* werden für UCC-Systeme derzeit nicht unterstützt.
- Die über CUPS eingebundenen Druckerfreigaben unterstützen nicht alle Kombinationen für Zugriffsberechtigungen. Das Freigeben aller Drucker über das Computerraum-Modul hat daher keine Auswirkung auf UCC-Systeme.
- Der Klassenarbeitsmodus von UCS@school wird auf UCC-Systemen nicht unterstützt.



Weitere Informationen zu UCC finden sich im UCC-Handbuch [ucc-handbuch].

## 12.1. Installation von UCC

 Feedback 

Im Folgenden wird die Installation von Univention Corporate Client (UCC) auf einem UCS@school-Schulserver beschrieben. Dabei wird die Kenntnis des UCC-Handbuchs [ucc-handbuch] vorausgesetzt und neben einer Kurzanleitung für die Installation nur abweichende Installationsschritte beschrieben.

Die Installation von UCC erfolgt über das Univention App Center in der Univention Management Console. Die Applikation *Univention Corporate Client* muss auf dem UCS@school-Schulserver installiert werden. Dies ist in einer Single-Server-Umgebung der Domänencontroller Master und in einer Multi-Server-Umgebung der Domänencontroller Slave. Die notwendigen Installationsschritte sind auf beiden UCS-Systemrollen gleich und werden daher im folgenden gemeinsam beschrieben. Vor der Installation von UCC muss zunächst die UCS@school-Umgebung fertig installiert und konfiguriert werden.


### Achtung

Die Verwendung von UCC in UCS@school setzt die Verwendung des offiziellen UCC-Desktop-Images oder eines selbsterstellten Desktop-Images voraus. Das offizielle UCC-Desktop-Image wird während der Installation vom Univention UCC-Repository-Server heruntergeladen und hat im gepackten Zustand eine Größe von ca. 3GB. Es ist daher, je nach Art und Geschwindigkeit der Internetanbindung, mit längeren Downloadzeiten zu rechnen. Nach erfolgreichem Download wird das Image entpackt. Daher muss vor der Installation von UCC auf dem Schulserver sichergestellt werden, dass mindestens mindestens 22 GB an freiem Speicherplatz vorhanden sind.

Auf dem Schulserver sind für die Installation von UCC die folgenden Schritte durchzuführen:

- Die Installation von UCC erfolgt über das Univention App Center. Dafür muss auf dem betreffenden System im Univention App Center die Applikation *Univention Corporate Client* ausgewählt und installiert werden.
- Nach Abschluss der App-Installation ist das offizielle UCC-Desktop-Image nachzuinstallieren. Die Installation des UCC-Desktop-Images kann im Univention App Center auf dem Reiter *Erweiterte Software-Verwaltung* erfolgen. Als Paketname ist **ucc-1.0-rev2-desktop-image** (oder eine neuere Version) für die Installation auszuwählen. Alternativ kann das Paket auf der Kommandozeile mit dem Befehl `univention-install ucc-1.0-rev2-desktop-image` installiert werden.
- Nach Abschluss der Installation von UCC und des UCC-Desktop-Images sind ggf. neue Joinskripte auf dem System installiert worden, die noch nicht ausgeführt wurden. Daher ist es wichtig, die noch nicht ausgeführten Joinskripte jetzt über das UMC-Modul *Domänenbeitritt* zu starten. Alternativ kann das Starten der Joinskripte auch auf der Kommandozeile über den Befehl `univention-run-join-scripts` erfolgen.

## 12.2. Konfigurationseinstellungen für UCC-Systeme

 Feedback 

Im Folgenden werden die UCS@school-spezifischen Konfigurationseinstellungen beschrieben, die von regulären UCC-Systemen abweichen. Weitergehende Konfigurationsmöglichkeiten werden im UCC-Handbuch [ucc-handbuch] beschrieben.

Für die korrekte Funktion der UCC-Systeme ist sicherzustellen, dass die UCC-Systeme den Domänencontroller Master (nur bei Single-Server-Umgebungen!) bzw. den Domänencontroller Slave (Multi-Server-Umgebung) als DNS-Server verwenden. In der Standardeinstellung wird automatisch eine DHCP-DNS-Richtlinie `cn=dhcp-dns-SCHULNAME,cn=policies,ou=SCHULNAME,dc=example,dc=com` erstellt und mit dem Container `cn=dhcp,ou=SCHULNAME,dc=example,dc=com` verknüpft, die die IP-Adresse des Schulservers als DNS-Server über DHCP konfiguriert. Das automatische Erstellen und Verknüpfen der DHCP-DNS-Richtlinie kann durch das Setzen der UCR-Variable `ucsschool/import/generate/policy/dhcp/dns/`



`set_per_ou=false` auf Domänencontroller Master- und Domänencontroller Slave-Systemen deaktiviert werden.


Die Konfiguration der UCC-Systeme erfolgt in der Standardeinstellung über eine automatisch vom Schulserver generierte UCR-Richtlinie. Diese trägt den Namen `ou-default-ucr-policy` und wird für jede Schul-OU unter dem DN `cn=ou-default-ucr-policy,cn=policies,ou=SCHULNAME,dc=example,dc=com` im LDAP-Verzeichnis abgelegt. Diese UCR-Richtlinie wird automatisch bei der Installation des Schulservers mit geeigneten Werten vordefiniert, welche nachfolgend beschrieben werden:

- Die UCR-Variable `ucc/mount/cifshome/server` definiert den Server, von dem das Samba-Heimatverzeichnis des sich anmeldenden Benutzers gemountet wird. In der Variable ist der FQDN anzugeben (Beispiel: `ucc/mount/cifshome/server=schulserver1.example.com`).
- Analog zur aus UCS bereits bekannten UCR-Variable `proxy/http` kann über die Variable `ucc/proxy/http` der HTTP-Proxy für die UCC-Systeme definiert werden (Beispiel: `ucc/proxy/http=http://schulserver1.example.com:3128`).
- Der CUPS-Druckserver für UCC-Systeme wird über die UCR-Variable `ucc/cups/server` festgelegt. Auch hier ist der FQDN des Druckservers anzugeben (Beispiel: `ucc/cups/server=schulserver1.example.com`).
- Für die Verwendung von iTALC wird auf den UCC-Systemen der iTALC-Schlüssel des Schulservers zur automatischen Authentifizierung benötigt. Die folgenden zwei Variablen definieren eine Samba-Freigabe sowie den Dateinamen der iTALC-Schlüsseldatei, über die das UCC-System die Schlüsseldatei beziehen kann: `ucc/italc/key/sambasource` und `ucc/italc/key/filename`. In der Standardeinstellung wird der iTALC-Schlüssel auf der `netlogon`-Freigabe des Schulservers abgelegt. Die Schlüsseldatei enthält dabei den Namen des Schulservers (Beispiel: `ucc/italc/key/sambasource=\\schulserver1\netlogon` und `ucc/italc/key/filename=italc-key_schulserver1.pub`).

Das automatische Erstellen und Verknüpfen der UCR-Richtlinie `ou-default-ucr-policy` kann durch das Setzen der UCR-Variable `ucsschool/import/generate/policy/ucc/settings=false` auf Domänencontroller Master- und Domänencontroller Slave-Systemen deaktiviert werden.

Die UCC-Systeme können Kerberos als Authentifizierungsmethode für die transparente Authentifizierung gegenüber dem HTTP-Proxy (squid) des Schulservers verwenden. Diese Authentifizierungsmethode ist in der Standardeinstellung im HTTP-Proxy des Schulservers deaktiviert und muss manuell durch das Setzen der Univention Configuration Registry-Variablen `squid/krb5auth=yes` aktiviert werden. Anschließend ist auf dem Schulserver ein Neustart des Dienstes `squid` notwendig, der entweder über das UMC-Modul `Systemdienste` oder auf der Kommandozeile über das Kommando `invoke-rc.d squid3 restart` durchgeführt werden kann.

## 12.3. Ausrollen von neuen UCC-Systemen

Feedback 

Sind Installation und Konfiguration von UCC auf dem Schulserver abgeschlossen, können neue UCC-Desktop-Systeme installiert und für `UCS@school` eingerichtet werden. Die nachfolgenden Schritte für den Rollout wurden auf ein Minimum reduziert und beinhalten abweichende Schritte zum regulären UCC-Rollout. Hinweise zu Rollout und Konfiguration von UCC-Desktop-Systemen können dem UCC-Handbuch [`ucc-handbuch`] entnommen werden.

- Für die Installation eines UCC-Desktop-Systems muss zunächst für jedes zu installierende System ein UCC-Objekt im LDAP-Verzeichnis erstellt werden. Hierzu werden Angaben wie IP-Adresse und MAC-Adresse benötigt. Das UCC-Objekt muss entweder in der Univention Management Console über das Modul `Computer hinzufügen` oder auf der Kommandozeile über das `UCS@school`-Importskript `import_computer` angelegt werden. Bei beiden Varianten ist darauf zu achten, dass als Rechnername `Univention Corpora-`

te *Client* bzw. *ucc* angegeben wird. Hinweise zum Importskript `import_computer` finden sich in Abschnitt 5.4.2.

- Nach dem Anlegen des UCC-Objektes muss das Objekt in der Univention Management Console geöffnet und auf den Reiter *Images* gewechselt werden. Dort sollte als Startvariante *Image-Boot mit Update-Prüfung / Erstinstallation*, das gewünschte UCC-Desktop-Image sowie *Neupartitionierung für installierte Systeme* ausgewählt werden. Diese Einstellungen beziehen sich ausschließlich auf den erstmaligen Rollout des UCC-Images auf ein neues System. Dabei werden alle vorhandenen Daten des Systems überschrieben.
- Die Installation der notwendigen Integrationspakete auf dem UCC-System kann manuell auf der Kommandozeile des UCC-Systems erfolgen (`apt-get install univention-ucc-ucsschool-integration`). Sollen mehrere UCC-Systeme ausgerollt werden, wird empfohlen, am Container `cn=computers,ou=SCHULNAME,dc=example,dc=com` eine neue Richtlinie vom Typ *UCC Software-Update-Einstellungen* zu verknüpfen, über die das Paket ***univention-ucc-ucsschool-integration*** automatisch beim Systemstart installiert wird.
- Wurden die vorgenannten Schritte durchgeführt, kann das UCC-System gestartet werden. Während des PXE-Boot-Vorgangs wird automatisch eine Repartitionierung und die Installation des UCC-Desktop-Images vorgenommen. Dabei werden vom UCC-System Informationen für den Domänenbeitritt abgefragt. Sofern die oben genannte Richtlinie eingerichtet wurde, wird beim Starten des UCC-Systems das Integrationspaket nachinstalliert.

## Achtung

Für die Nachinstallation des Integrationspakets muss das UCC-System Zugriff auf die offiziellen Univention-UCC-Repository-Server erhalten. Die dafür notwendigen DHCP-Routing-Einstellungen müssen ggf. vor dem ersten Bootvorgang eingerichtet werden.

- Nach Abschluss der manuellen bzw. automatischen Installation des Integrationspakets müssen einmalig auf dem UCC-System noch nicht ausgeführte Joinskripte aufgerufen werden. Dazu ist auf dem UCC-System auf der Kommandozeile der Befehl `univention-run-join-scripts` auszuführen. Dabei wird z.B. der iTALC-Schlüssel vom Schulserver auf das UCC-System kopiert.
- Zum Abschluss sollte das UCC-System neu gestartet werden.

# Literaturverzeichnis

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

[ucc-handbuch] Univention GmbH. 2013. *Univention Corporate Client - Manual for administrators*. <http://docs.univention.de/ucc-manual.html>.

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

