

UCS 4.2-1 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung
von Univention Corporate Server (UCS) 4.2-1**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2017 Univention GmbH

Mary-Somerville-Straße 1, 28359 Bremen, Deutschland/Germany

<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. Release-Highlights	4
2. Hinweise zum Update	5
2.1. Empfohlene Update-Reihenfolge	5
2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante	5
3. Vorbereitung des Updates	6
4. Nachbereitung des Updates	7
5. Hinweise zum Einsatz einzelner Pakete	8
5.1. Erfassung von Nutzungsstatistiken	8
5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit	8
5.3. Empfohlene Browser für den Zugriff auf Univention Management Console	8
6. Changelog	9
6.1. General	9
6.2. Univention Installer	9
6.3. Domain services	9
6.3.1. OpenLDAP	9
6.3.1.1. LDAP schema changes	9
6.3.1.2. Listener/Notifier domain replication	9
6.4. Univention Management Console	9
6.4.1. Univention Management Console web interface	9
6.4.2. Univention Portal	9
6.4.3. Univention Management Console server	10
6.4.4. Univention App Center	10
6.4.5. Univention Directory Manager UMC modules and command line interface	11
6.4.6. Modules for system settings / setup wizard	11
6.4.7. Mail	11
6.5. Software deployment	12
6.6. Univention base libraries	12
6.7. System services	12
6.7.1. Univention self service	12
6.7.2. Mail services	12
6.7.3. Printing services	13
6.7.4. Nagios	13
6.7.5. Kerberos	13
6.7.6. Proxy services	13
6.7.7. Apache	13
6.7.8. Radius	13
6.8. Virtualization	13
6.8.1. Univention Virtual Machine Manager (UVMM)	13
6.9. Services for Windows	13
6.9.1. Samba	13
6.9.2. Univention AD Takeover	14
6.9.3. Univention S4 Connector	14
6.10. Other changes	14

Kapitel 1. Release-Highlights


Mit Univention Corporate Server 4.2-1 steht das erste Point-Release für Univention Corporate Server (UCS) zur Verfügung. Es umfasst eine Reihe Funktionserweiterungen und Verbesserungen, neue Eigenschaften sowie diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Eine Weiterleitung der E-Mails kann nun pro Mailbenutzer im Managementsystem hinterlegt werden.
- Das Ändern des Passworts an UMC wurde verbessert. So können nun auch Benutzer aus einer Microsoft Active Directory Domänen ihr abgelaufenes Passwort ändern. Zusätzlich werden mehr Hinweise angezeigt, falls die Passwort Änderung fehlschlägt.
- Die IPv6 Konfigurationsmöglichkeiten diverser Dienste wurde verbessert, bspw. in der Nagios oder Proxy Server Konfiguration und im Managementsystem.

Kapitel 2. Hinweise zum Update

Während der Aktualisierung kann es zu temporären Ausfällen von Diensten innerhalb der Domäne kommen. Aus diesem Grund sollte das Update innerhalb eines Wartungsfensters erfolgen. Grundsätzlich wird empfohlen, das Update zunächst in einer Testumgebung einzuspielen und zu testen. Die Testumgebung sollte dabei identisch zur Produktivumgebung sein. Je nach Systemgeschwindigkeit, Netzwerkanbindung und installierter Software kann das Update zwischen 20 Minuten und mehreren Stunden dauern.


2.1. Empfohlene Update-Reihenfolge

Feedback 

In Umgebungen mit mehr als einem UCS-System muss die Update-Reihenfolge der UCS-Systeme beachtet werden:

Auf dem Domänencontroller Master wird die maßgebliche (authoritative) Version des LDAP-Verzeichnisdienstes vorgehalten, die an alle übrigen LDAP-Server der UCS-Domäne repliziert wird. Da bei Release-Updates Veränderungen an den LDAP-Schemata auftreten können, muss der Domänencontroller Master bei einem Release-Update immer als erstes System aktualisiert werden.

2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante

Feedback 

UCS-Installations-DVDs werden ab UCS 4 nur noch für 64-Bit-Architekturen bereitgestellt. Vorhandene 32-Bit UCS 3 Systeme können weiterhin über das Online Repository oder über Update DVDs auf UCS 4 aktualisiert werden. Die 32-Bit-Architektur wird für die gesamte UCS 4 Maintenance noch unterstützt.

Kapitel 3. Vorbereitung des Updates

Es sollte geprüft werden, ob ausreichend Festplattenplatz verfügbar ist. Eine Standard-Installation benötigt min. 6 GB Speicherplatz. Das Update benötigt je nach Umfang der vorhanden Installation ungefähr 1 GB weiteren Speicherplatz zum Herunterladen und Installieren der Pakete.

Für das Update sollte eine Anmeldung auf der lokalen Konsole des Systems mit dem Benutzer `root` durchgeführt und das Update dort gestartet werden. Alternativ kann das Update über Univention Management Console durchgeführt werden.

Eine Remote-Aktualisierung über SSH wird nicht empfohlen, da dies beispielsweise bei Unterbrechung der Netzverbindung zum Abbruch des Update-Vorgangs und zu einer Beeinträchtigung des Systems führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, dass das Update bei Unterbrechung der Netzverbindung trotzdem weiterläuft. Hierfür können beispielsweise die Tools `screen` oder `at` eingesetzt werden, die auf allen UCS Systemrollen installiert sind.


Kapitel 4. Nachbereitung des Updates

Nach dem Update müssen die neuen oder aktualisierten Join-Skripte ausgeführt werden. Dies kann auf zwei Wegen erfolgen: Entweder über das UMC-Modul **Domänenbeitritt** oder durch Aufruf des Befehls `univention-run-join-scripts` als Benutzer `root`.

Anschließend muss das UCS-System neu gestartet werden.

Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Erfassung von Nutzungsstatistiken


Feedback 

Bei Verwendung der UCS Core Edition (die in der Regel für Evaluationen von UCS herangezogen wird) werden anonyme Nutzungsstatistiken zur Verwendung von Univention Management Console erzeugt. Die aufgerufenen Module werden dabei von einer Instanz des Web-Traffic-Analyse-Tools Piwik protokolliert. Dies ermöglicht es Univention die Entwicklung von Univention Management Console besser auf das Kundeninteresse zuzuschneiden und Usability-Verbesserungen vorzunehmen.

Diese Protokollierung erfolgt nur bei Verwendung der UCS Core Edition. Der Lizenzstatus kann überprüft werden durch den Eintrag **Lizenz** -> **Lizenzinformation** des Benutzermenüs in der rechten, oberen Ecke von Univention Management Console. Steht hier unter **Lizenztyp** der Eintrag **UCS Core Edition** wird eine solche Edition verwendet. Bei Einsatz einer regulären UCS-Lizenz erfolgt keine Teilnahme an der Nutzungsstatistik.


Die Protokollierung kann unabhängig von der verwendeten Lizenz durch Setzen der Univention Configuration Registry-Variable `umc/web/piwik` auf `false` deaktiviert werden.

5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit

Feedback 

WebKit, Konqueror und QtWebKit werden in UCS im maintained-Zweig des Repositorys mitgeliefert, aber nicht durch Sicherheits-Updates unterstützt. WebKit wird vor allem für die Darstellung von HTML-Hilfeseiten u.ä. verwendet. Als Web-Browser sollte Firefox eingesetzt werden.

5.3. Empfohlene Browser für den Zugriff auf Univention Management Console

Feedback 

Univention Management Console verwendet für die Darstellung der Web-Oberfläche zahlreiche JavaScript- und CSS-Funktionen. Cookies müssen im Browser zugelassen sein. Die folgenden Browser werden empfohlen:


- Chrome ab Version 37
- Firefox ab Version 38
- Internet Explorer ab Version 11
- Safari und Safari Mobile ab Version 9

Auf älteren Browsern können Darstellungs- oder Performanceprobleme auftreten.

Kapitel 6. Changelog


Die Changelogs mit den detaillierten Änderungsinformationen werden nur in Englisch gepflegt. Aufgeführt sind die Änderungen seit UCS 4.2-0:

6.1. General

Feedback 


- All security updates issued for UCS 4.2-0 are included:
 - *samba* (CVE-2017-7494) (Bug 44612).
 - *openssl* (CVE-2016-7055 CVE-2016-8610 CVE-2017-3731 CVE-2017-3732) (Bug 44751).
 - *python-cryptography* (CVE-2016-9243) (Bug 44741).

6.2. Univention Installer


Feedback 

- The configuration file of *univention-net-installer* has been upgraded to use the Apache 2.4 syntax (Bug 44213).


6.3. Domain services

Feedback 

6.3.1. OpenLDAP


Feedback 

6.3.1.1. LDAP schema changes

Feedback 


- The LDAP scheme has been expanded by additional LDAP attributes to add support for forwarding user emails to external addresses (Bug 42249).
- The possibility to change the font color on the portal page has been added (Bug 44697).

6.3.1.2. Listener/Notifier domain replication


Feedback 

- The BDB cache is now migrated to MDB in case it didn't happen during update (Bug 44466).

6.4. Univention Management Console


Feedback 

6.4.1. Univention Management Console web interface

Feedback 


- Values inside of grids are now sorted locale aware (Bug 44361).
- Allow UMC feedback dialog for non traceback errors (Bug 44527).
- The link to send feedback to Univention has been fixed (Bug 44381).
- The way a grid is sorted is now better configurable for module developers (Bug 44652).
- Progress bars are now escaping HTML content more strict (Bug 44498).

6.4.2. Univention Portal

Feedback 

- The possibility to change the font color on the portal page has been added (Bug 44697).

6.4.3. Univention Management Console server

Feedback 


- The reason why changing the password failed is shown again (Bug 41786).
- An error during login via SAML has been fixed (Bug 44217).
- A redirection loop during SAML login is prevented (Bug 44450).
- The PAM configuration has been adjusted to make password changes possible again if the password was expired (Bug 43859).
- The error handling on module initialization has been improved (Bug 44428).
- If the URL to access UMC contained a port a XSRF attack was wrong detected causing UMC to be unusable. This has been fixed (Bug 44564).
- The link to send feedback to Univention has been fixed (Bug 44381).
- A crash of the UMC server during handling of errors has been fixed (Bug 44365).
- A notification about the Administrator account is shown when trying to login as root (Bug 40986).
- After a failed attempt to change an expired user password via the login dialog the form fields weren't reset resulting in further authentication attempts being impossible (Bug 44720).

6.4.4. Univention App Center

Feedback 


- The App Center now uses a different directory for special temporary files for Docker Apps to avoid problems with the System V init *tmp* cleanup (Bug 44501).
- During the remove of Docker Apps, the App is stopped via the init script (Bug 44286).
- Error handling has been improved (Bug 44493).
- Some Docker Apps did not register their user management extensions properly. This has been fixed (Bug 44550).
- Handle errors for package manager lock during docker installation in UMC (Bug 41303)
- Handle *BadStatusLine* line error (Bug 34543).
- Admin credentials are now passed to a preinst script during App installation / upgrade (Bug 44654).
- Progress bars are now escaping HTML content more strict (Bug 44498).
- Start containers with the hosts proxy settings by default (Bug 44561).
- A script can now be run after configuring an App (Bug 44750).
- Under certain circumstances, it was possible that the CLI selected the wrong App version. This issue has been fixed (Bug 44724).
- *AdditionalPackages* defined by the App are no longer removed when uninstalling an app (Bug 44778).
- The cron job for the updater check has been deactivated in *univention-docker-container-mode* (Bug 44630).
- A template for Docker proxy settings has been added (Bug 44536).

6.4.5. Univention Directory Manager UMC modules and command line interface

Feedback 


- The unmaintained and deprecated internal test suite has been removed (Bug 27286).
- Fix handling of "Change password on next login" for new user accounts (Bug 42148).
- Support for forwarding user emails to external addresses has been added (Bug 42249).
- The error handling regarding LDAP size limits has been improved (Bug 42533).
- Creating computers with IPv6 addresses is possible again (Bug 44152).
- Fix typo in users module when reading the minimal password length (Bug 44472).
- The default value of extended attributes which don't define any default has been changed from an empty string to None (Bug 41053).
- A regression in UCS 4.2 has been fixed which caused that DHCP pools which have values unknown by UDM in its *dhcpPermitList* could not be opened or modified anymore (Bug 44611).
- The font color on the portal page can be configured now (Bug 44697).
- Default values (especially from extended attributes) are now pre filled when modifying objects (Bug 41053).

6.4.6. Modules for system settings / setup wizard

Feedback 


- The AWS Apache start site link has been corrected (Bug 42133).
- The package *univention-self-service-master* is now also downloaded while preparing an appliance (Bug 44284).
- The package *univention-samba* is now also downloaded while preparing an appliance (Bug 44522).
- A cleanup script used in Univention App Appliances has been adapted for UCS 4.2 (Bug 44575).
- IP address changes are now also applied to portal entries (Bug 43671).
- When selecting fast demo mode in an App Appliance, all IP addresses in LDAP are reconfigured to the correct address (Bug 43140).
- The overview of changed network settings doesn't show HTML code anymore (Bug 41204).
- The decision between joining systems into UCS or Active Directory domains was confusing and has been improved (Bug 44035).
- A crash is prevented when trying to join into an Active Directory domain and the Active Directory server is not reachable (Bug 44394).
- A crash is prevented in appliance scenarios if no domain name was entered (Bug 43273).

6.4.7. Mail

Feedback 

- The UMC module System services showed the Cyrus IMAP service always as stopped. It does now show the correct service state. This issue has been fixed (Bug 44594).

6.5. Software deployment

Feedback 

- The file containing the APT repository during a UCS release update is no longer deleted on failures to allow fixing failed updates more easily (Bug 44346).
- A check to deny update on UCS member servers with the package slapd has been added to the updater preup script (Bug 44650)

6.6. Univention base libraries


Feedback 

- Make DNS lookup more robust for Kerberos `kinit` in `admember.check_ad_account` (Bug 38285).
- Handle `NoAnswer` exception of `dns.resolver` when looking for `_domaincontroller_master._tcp` SRV record during Active Directory member setup (Bug 38788).
- Properly stop Samba before running the Active Directory member setup (Bug 44144).
- The re-connecting methods for add and modify of python LDAP are used to better handle `SERVER_DOWN` conditions (Bug 44316).

6.7. System services


Feedback 

6.7.1. Univention self service

Feedback 

- The `memcache` service for the self service module did not start, because it was misconfigured. This issue has been fixed (Bug 44477).


6.7.2. Mail services

Feedback 

- The Fetchmail password attributes now disallows substring searches and are not searchable in UMC anymore (Bug 41336).
- The Fetchmail ACLs now respect overridden default group names (Bug 33648).
- After an upgrade from UCS 4.1 to UCS 4.2 the Cyrus daemons did not start automatically anymore. When installing this update the service will be enabled automatically in `systemd` (Bug 44377).
- The paths to Cyrus executables have been adjusted for Debian Jessie (Bug 44424, Bug 44566).
- The path to the tool to automatically purge old entries from the Cyrus "duplicate delivery database" has been fixed. As the path was wrong in the past, the tool never ran. When starting it (the first time), it may take minutes or hours (depending on the database size). Via the new Univention Configuration variables `mail/cyrus/duplicate-supression/expiry/start` and `mail/cyrus/duplicate-supression/expiry/event` this cleanup job can be configured to be run when starting Cyrus or regularly at 4:01 each night (Bug 22852).
- The package dependencies allow now to install Dovecot Pro instead of Dovecot from the UCS repositories (Bug 44559).
- Support for forwarding user emails to external addresses has been added. During the update, the Univention Configuration variables `mail/postfix/virtual/alias/maps` and `mail/postfix/virtual/mailbox/maps` are updated automatically, because some postfix virtual lookup tables have been modified. Please note, that the forwarding of emails on systems with OX App Suite will only come into effect if at least version 7.8.3-ucs2 of OX App Suite is installed (Bug 42249).
- The default of the UCR variable `mail/postfix/tls/client/level` when unset has been changed to "may". On existing UCS installations this has already been set explicitly (Bug 44589).


- When a relay host with authentication is used (*mail/relayauth=yes*), the Postfix option *smtp_tls_security_level* will automatically be set to "encrypt", unless *mail/postfix/tls/client/level* is set to "none" (Bug 44589).
- Entries in the SMTP client TLS policy table can now be configured for each domain or mail exchanger individually through the UCR variables *mail/postfix/tls/client/policy/.** (Bug 44811).

6.7.3. Printing services

Feedback 


- Samba is now reloaded after printer has been created (Bug 44153).

6.7.4. Nagios

Feedback 


- IPv6 support for allowed hosts has been added (Bug 44454).

6.7.5. Kerberos

Feedback 


- User accounts from Active Directory are now able to change their expired password via UMC (Bug 43859).

6.7.6. Proxy services

Feedback 


- When switching to UCS 4.2 the program name of squid's Kerberos authentication handler has changed. The authentication helper of *univention-squid* has been changed accordingly (Bug 44287).
- Allow IPv6 addresses in UCR variable *squid/allowfrom* (Bug 29576).

6.7.7. Apache

Feedback 


- Exceptions for the *apache2/force_https* configuration can now be configured via UCR. When *apache2/force_https* is enabled, by default "localhost" will be excluded (Bug 44628)

6.7.8. Radius


Feedback 

- Allow *TTLs* to be disabled via UCR *freeradius/conf/auth-type/ttls* (Bug 42728)
- Allow the ports the server listens on to be configured via UCR *freeradius/conf/port* and *freeradius/conf/accountingport* (Bug 42729).
- Allow the maximum number of requests which the server keeps track of to be configured via UCR *freeradius/conf/max_requests* (Bug 42730).

6.8. Virtualization


Feedback 

6.8.1. Univention Virtual Machine Manager (UVMM)


Feedback 

- The unused PAM access file has been removed (Bug 33702).

6.9. Services for Windows

Feedback 


6.9.1. Samba

Feedback 

- The UCR variable *samba/idmap/range* has been added to configure the *uid* and *gid* range for the default (*) *idmap* backend. This can be used to avoid overlaps between that default range and the domain specific setting, which is configurable via *samba/idmap/\$windows_domain/range* (Bug 44549).


- The UCR variables `samba/client/min/protocol`, `samba/min/protocol` and `samba/client/max/protocol` have been added. Please be aware that raising `samba/min/protocol` e.g. to SMB2 also requires raising `samba/client/max/protocol` to that value or higher (Bug 44591).
- Improve handling of *tombstoned* DNS objects during *DDNS* update (Bug 39806).
- Keep `DNS_TYPE_TOMBSTONE` value marker and `dnsTombstoned` attribute in sync (Bug 39806).
- Allow *DDNS* update if the account name of authenticated machine matches the name of the target record (Bug 41190).
- Don't fail join if *CNF* objects are in *serverReferenceBL* (Bug 43280)
- Don't consider unreachable UCS@school Slave DCs for joining (Bug 43478)
- Support uppercase *CN* attribute in `sysvol-cleanup.py` (Bug 43620)
- Adjust `check_essential_samba4_dns_records.sh` to change of behavior of the `host` command in UCS 4.2 (Bug 44535)
- The UCR variables `samba/client/min/protocol`, `samba/min/protocol` and `samba/client/max/protocol` have been added. Please be aware that raising `samba/min/protocol` e.g. to SMB2 also requires raising `samba/client/max/protocol` to that value or higher (Bug 44643).
- Make `sysvol-sync.sh` robust against varying *stderr* output from `rsync` (Bug 44694).
- Update Samba package and restart BIND9 on upgrade to make BIND9 load the updated `dlz_bind9` module version, which contains improvements in the handling of *DDNS* updates (Bug 39806, Bug 41190).

6.9.2. Univention AD Takeover

 Feedback 


- Avoid traceback in case AD Takeover is run in AD member mode (Bug 38983).

6.9.3. Univention S4 Connector

 Feedback 

- Fix fetching the SID in `sync_from_ucs ALREADY_EXISTS` handling (Bug 43368)
- Fix handling special case of *Printer-Admins* (Bug 44276)
- Fix the handling of UTF-8 encoded DN's (Bug 44276)
- Don't append a trailing dot to DNS alias values if there is no dot (Bug 31311).
- Allow removal of specific sub-objects objects in `sync_from_ucs` (Bug 33882).
- Don't consider unreachable UCS@school Slave DCs when looking for hosts (Bug 43478). running a S4-Connector
- Fix handling of *Printer-Admins* (Bug 44517).

6.10. Other changes

 Feedback 

- The KDM init script now waits for the stop of the plymouth boot splash before starting and presenting the KDE login window (Bug 44452).
- A symbolic link has been added to enable *debootstrap* for UCS 4.2 (Bug 44593).

- All *postgresql-9.4* packages are now available in UCS 4.2 (Bug 44507).
- Missing French translations have been updated (Bug 44133).
- Removed the App re-registration during the upgrade to UCS 4.2-1. This was only necessary for upgrades to UCS 4.2-0 (Bug 44812).