

## UCS 4.4 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung  
von Univention Corporate Server (UCS) 4.4-7**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2020 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. Domain services .....	11
6.2.1. OpenLDAP .....	11
6.2.1.1. Listener/Notifier domain replication .....	11
6.3. Univention Management Console .....	11
6.3.1. Univention Management Console web interface .....	11
6.3.2. Univention Portal .....	11
6.3.3. Univention Management Console server .....	11
6.3.4. Univention App Center .....	12
6.3.5. Univention Directory Manager UMC modules and command line interface .....	12
6.3.6. Modules for system settings / setup wizard .....	12
6.3.7. Domain join module .....	13
6.3.8. System diagnostic module .....	13
6.3.9. Other modules .....	13
6.4. Univention base libraries .....	13
6.5. Software deployment .....	13
6.6. System services .....	13
6.6.1. SAML .....	13
6.6.2. Univention self service .....	14
6.6.3. Mail services .....	14
6.6.4. Postfix .....	14
6.6.5. Apache .....	14
6.6.6. RADIUS .....	15
6.7. Services for Windows .....	15
6.7.1. Samba .....	15
6.7.2. Univention S4 Connector .....	15
6.7.3. Univention Active Directory Connection .....	15
6.8. Other changes .....	15

# Kapitel 1. Release-Highlights


Mit Univention Corporate Server 4.4-7 steht das siebte Point-Release für Univention Corporate Server (UCS) 4.4 zur Verfügung. Es umfasst Funktionserweiterungen und Verbesserungen, neue Eigenschaften sowie diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Das Bearbeiten der eigenen Kontaktinformationen am UCS *Self Service* ist mit bestehender Single Sign On Anmeldung möglich.
- Administratoren können über die UCR Variable `umc/cookie-banner/show` die Anzeige eines Banners steuern, dass Benutzer über die Verwendung von Cookies bei der Benutzung des UCS Portals und weiterer Dienste informiert.
- Im S4 Connector und im AD Connector wurde ein Bug behoben, der nach dem Verschieben oder Deaktivieren von Benutzerobjekten diese Objekte noch in für sie nicht mehr relevanten Gruppen zugeordnet hat.
- Das Update auf Samba 4.10.18 entschärft die *Zerologon* Lücke, neue Optionen ermöglichen die sichere Konfiguration in Umgebungen, in denen *Secure Channel* verwendet werden muss.
- Diverse Security Updates wurden in UCS 4.4-7 integriert, bspw. für Postgresql, Samba, den Linux Kernel und PHP. Eine vollständige Liste von Security- und Paketupdates ist in Kapitel 6 zu finden.

## 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. 10 GB Speicherplatz. Das Update benötigt je nach Umfang der vorhanden Installation ungefähr 4 GB zusätzlichen 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.

Univention bietet ein Skript an, mit dem Probleme, die das Update des UCS Systems verhindern würden, schon vor dem Update erkannt werden können. Dieses Skript kann vor dem Update manuell auf das System geladen und ausgeführt werden:

```
# download
curl -Oos https://updates.software-univention.de/download/univention-
update-checks/pre-update-checks-4.4{,.gpg}

# run script
gpgv --keyring /usr/share/keyrings/univention-archive-key-ucs-4x.gpg \
  pre-update-checks-4.4.gpg \
    pre-update-checks-4.4 && bash pre-update-checks-4.4

...

Starting pre-update checks ...

Checking app_appliance ... OK
Checking block_update_of_NT_DC ... OK
Checking cyrus_integration ... OK
Checking disk_space ... OK
Checking hold_packages ... OK
Checking ldap_connection ... OK
Checking ldap_schema ... OK
...
```


## 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 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 71
- Firefox ab Version 60
- Safari und Safari Mobile ab Version 12
- Microsoft Edge ab Version 18

Der Internet Explorer wird ab diesem Release nicht mehr von Univention Management Console unterstützt.


Mit 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 4.4-6:

## 6.1. General


Feedback 

- All security updates issued for UCS 4.4-6 are included:
  - *bluez* (CVE-2020-27153) (Bug 52265)
  - *curl* (CVE-2020-8231) (Bug 52142)
  - *firefox-esr* (CVE-2020-15673 CVE-2020-15676 CVE-2020-15677 CVE-2020-15678 CVE-2020-15683 CVE-2020-15969 CVE-2020-16012 CVE-2020-26950 CVE-2020-26951 CVE-2020-26953 CVE-2020-26956 CVE-2020-26958 CVE-2020-26959 CVE-2020-26960 CVE-2020-26961 CVE-2020-26965 CVE-2020-26968) (Bug 52160 Bug 52266 Bug 52352 Bug 52414)
  - *firmware-nonfree* (CVE-2016-0801 CVE-2017-0561 CVE-2017-9417 CVE-2017-13077 CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081 CVE-2018-5383) (Bug 52420)
  - *freetype* (CVE-2020-15999) (Bug 52267)
  - *gdm3* (CVE-2020-16125) (Bug 52329)
  - *krb5* (CVE-2020-28196) (Bug 52325)
  - *libdbi-perl* (CVE-2019-20919 CVE-2020-14392 CVE-2020-14393) (Bug 52161)
  - *libexif* (CVE-2020-16125) (Bug 52329)
  - *libmaxminddb* (CVE-2020-28241) (Bug 52350)
  - *libonig* (CVE-2019-13224 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204 CVE-2019-19246 CVE-2020-26159) (Bug 52326)
  - *libproxy* (CVE-2020-26154) (Bug 52365)
  - *libsndfile* (CVE-2017-6892 CVE-2017-14245 CVE-2017-14246 CVE-2017-14634 CVE-2018-19661 CVE-2018-19662 CVE-2018-19758 CVE-2019-3832) (Bug 52288)
  - *libvirt* (Bug 52181)
  - *libvncserver* (CVE-2020-25708) (Bug 52366)
  - *linux* (CVE-2019-9445 CVE-2019-19073 CVE-2019-19074 CVE-2019-19448 CVE-2020-12351 CVE-2020-12352 CVE-2020-12655 CVE-2020-12771 CVE-2020-12888 CVE-2020-14305 CVE-2020-14314 CVE-2020-14331 CVE-2020-14356 CVE-2020-14386 CVE-2020-14390 CVE-2020-15393 CVE-2020-16166 CVE-2020-24490 CVE-2020-25211 CVE-2020-25212 CVE-2020-25220 CVE-2020-25284 CVE-2020-25285 CVE-2020-25641 CVE-2020-25643 CVE-2020-26088) (Bug 52287)
  - *lua5.3* (CVE-2020-24370) (Bug 52140)
  - *mariadb-10.1* (CVE-2020-15180) (Bug 52264)


- *nss* (CVE-2018-12404 CVE-2018-18508 CVE-2019-11719 CVE-2019-11729 CVE-2019-11745 CVE-2019-17006 CVE-2019-17007 CVE-2020-6829 CVE-2020-12399 CVE-2020-12400 CVE-2020-12401 CVE-2020-12402 CVE-2020-12403) (Bug 52190)
- *openjdk-8* (CVE-2020-14779 CVE-2020-14781 CVE-2020-14782 CVE-2020-14792 CVE-2020-14796 CVE-2020-14797 CVE-2020-14798 CVE-2020-14803) (Bug 52268)
- *openssl1.0* (CVE-2020-1968) (Bug 52141)
- *php7.0* (CVE-2020-7070) (Bug 52193)
- *poppler* (CVE-2017-14926 CVE-2017-14928 CVE-2018-19058 CVE-2018-20650 CVE-2018-20662 CVE-2019-7310 CVE-2019-9959 CVE-2019-10018 CVE-2019-14494) (Bug 52327)
- *postgresql-9.6* (CVE-2020-25694 CVE-2020-25695 CVE-2020-25696) (Bug 52400)
- *python3.5* (CVE-2019-20907 CVE-2020-26116) (Bug 52415)
- *qt4-x11* (CVE-2018-15518 CVE-2018-19869 CVE-2018-19870 CVE-2018-19871 CVE-2018-19872 CVE-2018-19873 CVE-2020-17507) (Bug 52139)
- *qtbse-opensource-src* (CVE-2018-19872 CVE-2020-17507) (Bug 52162)
- *qtsvg-opensource-src* (CVE-2018-19869) (Bug 52290)
- *raptor2* (CVE-2017-18926) (Bug 52328)
- *ruby2.3* (CVE-2020-25613) (Bug 52189)
- *samba* (CVE-2020-1472 CVE-2020-14318 CVE-2020-14323 CVE-2020-14383) (Bug 52130 Bug 52233)
- *sane-backends* (CVE-2020-12862 CVE-2020-12863 CVE-2020-12865 CVE-2020-12867) (Bug 51831)
- *spice* (CVE-2020-14355) (Bug 52291)
- *tcpdump* (CVE-2020-8037) (Bug 52351)
- *univention-kernel-image* (CVE-2019-9445 CVE-2019-19073 CVE-2019-19074 CVE-2019-19448 CVE-2020-12351 CVE-2020-12352 CVE-2020-12655 CVE-2020-12771 CVE-2020-12888 CVE-2020-14305 CVE-2020-14314 CVE-2020-14331 CVE-2020-14356 CVE-2020-14386 CVE-2020-14390 CVE-2020-15393 CVE-2020-16166 CVE-2020-24490 CVE-2020-25211 CVE-2020-25212 CVE-2020-25220 CVE-2020-25284 CVE-2020-25285 CVE-2020-25641 CVE-2020-25643 CVE-2020-26088) (Bug 52287)
- *univention-kernel-image-signed* (CVE-2019-9445 CVE-2019-19073 CVE-2019-19074 CVE-2019-19448 CVE-2020-12351 CVE-2020-12352 CVE-2020-12655 CVE-2020-12771 CVE-2020-12888 CVE-2020-14305 CVE-2020-14314 CVE-2020-14331 CVE-2020-14356 CVE-2020-14386 CVE-2020-14390 CVE-2020-15393 CVE-2020-16166 CVE-2020-24490 CVE-2020-25211 CVE-2020-25212 CVE-2020-25220 CVE-2020-25284 CVE-2020-25285 CVE-2020-25641 CVE-2020-25643 CVE-2020-26088) (Bug 52287)
- *wireshark* (CVE-2019-10894 CVE-2019-10895 CVE-2019-10896 CVE-2019-10899 CVE-2019-10901 CVE-2019-10903 CVE-2019-12295) (Bug 52289)
- *zeromq3* (CVE-2020-15166) (Bug 52349)

- The following updated packages from Debian Stretch 9.13 are included (Bug 52381): *php-pear, libdate-time-timezone-perl, linux-latest, tzdata, activemq, blueman, bouncycastle, cargo, cimg, dompurify.js, drupal7, eclipse-wtp, fastd, gcc-mozilla, golang-1.7, golang-1.8, golang-go.crypto, guacamole-server, httpcomponents-client, inspircd, jackson-databind, jruby, junit4, jupyter-notebook, linux-4.19, linux-latest-4.19, llvm-toolchain-7, mediawiki, moin, nfdump, nodejs-mozilla, obfs4proxy, pacemaker, packagekit, packer, phpmyadmin, puma, rails, rclone, restic, ruby-gon, ruby-json-jwt, ruby-rack-cors, rustcbindgen, rustc, sddm, snmptt, spice-gtk, sympa, thunderbird, tigervnc, tomcat8, wordpress, yaws, zabbix*


## 6.2. Domain services

Feedback 

### 6.2.1. OpenLDAP


Feedback 

#### 6.2.1.1. Listener/Notifier domain replication


Feedback 

- Setting *mdb maxsize* to 4GB (Bug 39167).

## 6.3. Univention Management Console


Feedback 

### 6.3.1. Univention Management Console web interface

Feedback 


- It is now possible to not download the `meta.json` from UMC, but the inexpensive one from Apache directly (Bug 52303).
- The interval for polling of session infos has been changed from every 30 seconds to the time the session will end to reduce network workload (Bug 52321).
- The cookie's path of the cookie banner is now valid for the whole domain (Bug 52222).
- A Cookie Banner can now be shown in the Portal and on the login page. It can be enabled by setting the UCR variable `umc/cookie-banner/show` to true (Bug 50302).

#### 6.3.2. Univention Portal

Feedback 

- The portal does not download the personalized `meta.json`, which would involve UMC. The portal does not need the additional information and may save one expensive request (Bug 52303).
- The groups that are considered as administrators can be configured via the new UCR variable ``portal/admin_groups'`. Only users of these groups do one additional check whether the edit mode is available. This should improve performance if many non admin users log in (Bug 52302).
- The evaluation whether or not a portal entry is visible now got a shortcut if the user is not logged in. This can improve the performance in certain situations considerably (Bug 52355).
- Fetching the portal entries is not done multiple times anymore if it is not expected that the contents changed through the edit mode (Bug 52345).
- A Cookie Banner can now be shown in the Portal and on the login page (Bug 50302).


#### 6.3.3. Univention Management Console server

Feedback 

- The SAML authentication at the UMC server has been deferred to the first use of an UMC module (Bug 52297).
- The SAML assertion lifetime is now configurable per service provider (Bug 52323).


- Fetching `/univention/get/meta` involves a call to UMC. This is not always necessary. Now it is possible to fetch a stripped down static version instead. This patch moves the meta file into a public folder (Bug 52303).
- To prevent connections between UMC web server and UMC server from being unexpectedly closed by a racing condition from the UMC server thus causing an error, handling of incoming connections in the UMC server has been improved. This problem previously only occurred in the new multi-process mode of the UMC server (Bug 52316).
- The UMC server now runs with an additional UNIX socket. The communication between UMC webserver and UMC server therefore does not need to be TLS encrypted anymore so that the performance is improved (Bug 52274).
- The interval for polling of session infos has been changed from every 30 seconds to the time the session will end to reduce network workload (Bug 52321).
- The UMC web server now sets the HTTP reason phrase for 503 Service Unavailable errors (Bug 52318).
- A memory optimization for SAML based sessions has been done in the UMC web server (Bug 52338).
- Only relevant information about the SAML response is stored in the session (Bug 52296).
- A log message has been removed which logged every session ID when cleaning up one session (Bug 52295).
- Objects stored in sessions now define Python `__slots__`, to minimize the used memory (Bug 52294).
- The regular interval for the processing of recurring tasks in the UMC server and UMC webserver can now be configured via UCR (Bug 52271).
- The performance during login at UMC has been improved by using the C implementation of *ElementTree* for parsing module and category definitions (Bug 52253).
- A Cookie Banner can now be shown in the Portal and on the login page (Bug 50302).
- Adjustments for the Self-Service have been added (Bug 51607).

### 6.3.4. Univention App Center

 Feedback 


- The UDM extension `appcenter/app` has been updated to be compatible to *python3*. The `joinscript` has been updated to specify a `--ucsversionend` option with the `ucs_registerLDAPExtension` calls. This is required in preparation for UCS 5.0 (Bug 52429).

### 6.3.5. Univention Directory Manager UMC modules and command line interface

 Feedback 

- An error while creating users with a `mailPrimaryAddress` has been corrected which occurred when the app "Open-Xchange" is installed (Bug 51907).
- User templates may now contain all attributes from the LDAP object class `inetOrgPerson` again (Bug 51364).
- The list of copyable user attributes has been updated. Several odd attributes have been removed, e.g. `first-name`, `lastname`, `jpegphoto` (Bug 49823).


### 6.3.6. Modules for system settings / setup wizard

 Feedback 

- The name of a specific `meta.json` file was changed. This change is internal (Bug 52303).


- Fix to adjust to new **firefox** behavior. The `userpref` option `toolkit.legacyUserProfileCustomizations.stylesheets` has to be set to `yes` in order to make **firefox** load the system setup specific file `userChrome.css` (Bug 52160).

### 6.3.7. Domain join module

Feedback 


- `univention-run-join-scripts` now validates command line arguments and does not run all scripts if an unknown parameter is given (Bug 46985).
- During the update from UCS 4.4 to UCS 5.0 the execution of `joinscripts` is postponed depending on the phase read from the updater status file. This change is a preparation for the upcoming update (Bug 51624).

### 6.3.8. System diagnostic module

Feedback 


- The usability of the `univention-run-diagnostic-checks` command line tool has been improved. It can now be called without parameters to execute all tests and it does not require a username and password to access `--help` any more (Bug 51942).

### 6.3.9. Other modules

Feedback 


- The users/user wizard can now be configured to enable the checkbox "Invite user via e-mail" by default via the UCR variable `directory/manager/web/modules/users/user/wizard/property/invite/default` (Bug 52046).

## 6.4. Univention base libraries

Feedback 


- The `ucs_registerLDAPExtension` offers an additional option `--name` which can be used to specify the RDN of the LDAP object. This can be useful if two versions of a UDM or LDAP extension need to be active simultaneously in the domain, e.g. one being only compatible to **python2**, but still required for UCS 4.4-based systems in the domain and another being only compatible to **python3**, required for the systems which at some point will have updated to UCS 5. This may be useful in preparation to the UCS 5.0 release (Bug 52433).
- Evaluation of ucr variables in the function `clean_old_backups` has been fixed (Bug 51765).
- Changing the value of the `ldap/database/mdb/maxsize` and `listener/cache/mdb/maxsize` variables to 4 GB (Bug 39167).
- Setting of ucr `backup/clean/max_age` variable for new installations with default 365 (Bug 51765).

## 6.5. Software deployment


Feedback 

- The status information "phase" has been added to the status file of the Univention Updater `/var/lib/univention-updater/univention-updater.status` (Bug 52197).
- Add command `univention-prune-kernels` to remove no longer needed kernel packages (Bug 51769).

## 6.6. System services

Feedback 


### 6.6.1. SAML

Feedback 

- The SAML assertion lifetime is now configurable per service provider (Bug 52323).


- The site does not download the personalized `meta.json`, which would involve UMC. The site does not need the additional information and may save one expensive request (Bug 52303).
- Two unnecessary LDAP bind calls have been deferred to when they are actually needed (Bug 52278).
- The file `/var/lib/simplesamlphp/secrets.inc.php` which contains the *simplesamlphp* administration password could be read by any local user (Bug 51922).
- Fix listener to set correct permissions for `/etc/simplesamlphp/serviceprovider_enabled_groups.json` This fixes a bug where SAML permissions applied to groups could not be evaluated (Bug 51608).
- The password change dialog was incorrectly shown even if an incorrect password was entered and the password was expired. This has been fixed (Bug 51903).

## 6.6.2. Univention self service

 Feedback 


- The point in time for token validity and rate limiting is now stored in UTC (Bug 52362).
- The token validity check has been repaired if the token was used one day later (Bug 52362).
- The UCR Variable `umc/self-service/passwordreset/token_validity_period` is now evaluated correctly (Bug 51287).
- The Self-Service module "Your Profile" can now be used while logged in (e.g via SAML) without re-entering credentials. The behavior will only be activated on new installations with UCS 4.4-7 and can be enabled manually by setting the UCR variable `umc/self-service/allow-authenticated-use` to true. When enabling the behavior all UCR variables for the Self-Service which are set on the DC Master must be set identically on the Self-Service System (Bug 51607).

## 6.6.3. Mail services

 Feedback 


- The joinscript of *univention-fetchmail* has been updated to specify a `--ucsversionend` option with the `ucs_registerLDAPExtension` calls. This is required in preparation for UCS 5.0 (Bug 52426).
- A new LDAP attribute was added to the mail schema for saving the new forwarding setting. For this, support was added for saving the mail forwarding setting in a dedicated LDAP attribute when UDM is used. In *univention-mail-postfix* support was added for using all LDAP query results for alias resolution, using a unionmap. This will be activated by default for all new installations. Existing installation must be manually migrated. Please refer to the upgrade instructions in: <https://help.univention.com/t/migration-of-ldap-attribute-mailforwardcopytoself/16509> (Bug 45205).

## 6.6.4. Postfix

 Feedback 

- The following UCR variables have been added for configuring Postfix: `mail/postfix/{maximal_queue_lifetime,bounce_queue_lifetime, delay_warning_time}` (Bug 51124).


## 6.6.5. Apache

 Feedback 

- Various Apache configurations may now be configured via UCR variables. See the UCR variable information for more details. ``apache2/min-spare-servers` `apache2/max-spare-servers`` (Bug 52320).
- Various Apache configurations may now be configured via UCR variables. See the UCR variable information for more details. `apache2/server-limit apache2/start-servers apache2/min-spare-threads apache2/max-spare-threads apache2/threads-per-child apa-`


`che2/server-signature` `apache2/server-tokens` `apache2/server-admin` (Bug 51294).

### 6.6.6. RADIUS


Feedback 

- The joinscript has been updated to specify a `--ucsversionend` option with the `ucs_registerLDAPExtension` calls. This is required in preparation for UCS 5.0 (Bug 52427).

## 6.7. Services for Windows


Feedback 

### 6.7.1. Samba

Feedback 


- The new UCR variable `create/spn/account/timeout` sets the timeout for how long the system waits for successful synchronization of the SPN account during a domain join. The default timeout has been increased to 10800s (Bug 51835).
- Samba has been adjusted so that disabling insecure DES encryption will not create any rejects in the `s4-connector` at user creation or password change any more (Bug 46745).

### 6.7.2. Univention S4 Connector

Feedback 


- The UDM extensions have been updated to be compatible to `python3`. The joinscript has been updated to specify a `--ucsversionend` option with the `ucs_registerLDAPExtension` calls. This is required in preparation for UCS 5.0 (Bug 52428).
- The group membership synchronization after moving objects has been fixed (Bug 52364).
- The S4 connector has been adjusted so that disabling insecure DES encryption types for Samba Kerberos will not create rejects on user creation or password change any more (Bug 46745).
- The synchronization of the `CN=Default Domain Policy,CN=System` container can now be enabled with the UCR variable `connector/s4/mapping/domainpolicy=yes`. The schema file `n_domain-policy.schema` has to be activated beforehand. See the manual for more information (Bug 51782).

### 6.7.3. Univention Active Directory Connection

Feedback 

- The AD Connector Mapping is now customizable via the file `/etc/univention/connector/localmapping.py`. The manual has details on how to write this file (Bug 49981).
- The group membership synchronization after moving objects has been fixed (Bug 51929).
- The flag `pwdChangeNextLogin` was incorrectly unset during the sync to UCS if the password was reset without changing the flag `pwdChangeNextLogin`. This behavior has been fixed (Bug 51501).
- If the transport connection is unexpectedly interrupted during a password synchronization, the AD connector will now reopen the connection and retry the sync (Bug 51904).

## 6.8. Other changes

Feedback 

- Expose LDAP extended error message (Bug 51903).