

UCS 5.0 Release Notes



**Release notes for the installation and update
of Univention Corporate Server (UCS) 5.0-2**

Publication date 2022-06-30

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2022 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.

Table of Contents

| | |
|--|----|
| 1. Release Highlights | 5 |
| 2. Notes about the update | 6 |
| 2.1. Recommended update order for environments with more than one UCS server | 6 |
| 2.2. UCS only available for 64 bit | 6 |
| 3. Simultaneous operation of UCS and Debian on UEFI systems | 7 |
| 4. Local package repository | 8 |
| 5. Preparation of update | 9 |
| 6. Postprocessing of the update | 10 |
| 7. Notes on selected packages | 11 |
| 7.1. Collection of usage statistics | 11 |
| 7.2. Recommended browsers for the access to Univention Management Console | 11 |
| 8. Changelog | 12 |
| 8.1. General | 12 |
| 8.2. Univention Installer | 14 |
| 8.3. Basic system services | 14 |
| 8.3.1. Univention Configuration Registry | 14 |
| 8.3.1.1. Changes to templates and modules | 14 |
| 8.4. Domain services | 15 |
| 8.4.1. OpenLDAP | 15 |
| 8.4.1.1. Listener/Notifier domain replication | 15 |
| 8.4.2. DNS server | 15 |
| 8.4.3. Univention Directory Listener | 15 |
| 8.5. Univention Management Console | 15 |
| 8.5.1. Univention Management Console web interface | 15 |
| 8.5.2. Univention Portal | 16 |
| 8.5.3. Univention Management Console server | 16 |
| 8.5.4. Univention App Center | 16 |
| 8.5.5. Univention Directory Manager UMC modules and command line interface | 17 |
| 8.5.6. Modules for system settings / setup wizard | 18 |
| 8.5.7. Domain join module | 18 |
| 8.5.8. Univention Directory Reports | 18 |
| 8.5.9. System diagnostic module | 18 |
| 8.5.10. Filesystem quota module | 19 |
| 8.5.11. Other modules | 19 |
| 8.6. Univention base libraries | 19 |
| 8.7. Software deployment | 20 |
| 8.8. System services | 20 |
| 8.8.1. PostgreSQL | 20 |
| 8.8.2. Docker | 20 |
| 8.8.3. SAML | 20 |
| 8.8.4. Univention self service | 20 |
| 8.8.5. Mail services | 21 |
| 8.8.6. Dovecot | 21 |
| 8.8.7. Postfix | 21 |
| 8.8.8. Monitoring / Nagios | 21 |
| 8.8.9. Apache | 21 |
| 8.8.10. RADIUS | 21 |
| 8.8.11. Proxy services | 21 |
| 8.8.12. Kerberos | 22 |
| 8.8.13. SSL | 22 |
| 8.8.14. DHCP server | 22 |
| 8.9. Services for Windows | 22 |

| | |
|---|----|
| 8.9.1. Samba | 22 |
| 8.9.2. Univention AD Takeover | 22 |
| 8.9.3. Univention S4 Connector | 23 |
| 8.9.4. Univention Active Directory Connection | 23 |
| 8.10. Other changes | 23 |
| Bibliography | 25 |

Chapter 1. Release Highlights


With Univention Corporate Server 5.0-2, the second point release for Univention Corporate Server (UCS) 5.0 is now available. It provides several feature improvements and extensions, new properties as well as various improvements and bugfixes. Here is an overview of the most important changes:

- The User Self Service was integrated into the UCS portal. Furthermore, the support for additional placeholders was extended among others, such as firstname and lastname in the email template for password reset.
- For RADIUS, users can assign a so-called service specific password. And administrators can assign dedicated VLANs to user groups to increase network security.
- *SameSite* Cookies can now be configured for UMC and SAML.
- The AD Takeover has been made more robust.
- Numerous performance improvements have been implemented regarding DNS, LDAP and during the sign in to UMC.
- The French translation for the UCS management system was updated.
- The UMC system diagnostics has been extended: Several new checks have been added and some older have been improved.
- Most packages have been migrated to Python 3. Their Python 2 counterparts are no longer installed by default and will be removed.
- This Univention Corporate Server release is based on Debian 10.12 *Buster*.
- Various security updates have been integrated into UCS 5.0-2, for example for Samba4, OpenLDAP, OpenSSL, and the Linux kernel.

Chapter 2. Notes about the update

During the update some services in the domain may not be available temporarily, that is why the update should occur in a maintenance window. It is recommended to test the update in a separate test environment prior to the actual update. The test environment should be identical to the production environment. Depending on the system performance, network connection and the installed software the update will take between 20 minutes and several hours. In large environments it may be useful to consult the [ucs-performance-guide].


2.1. Recommended update order for environments with more than one UCS server

Feedback 

In environments with more than one UCS system, the update order of the UCS systems must be borne in mind:

The authoritative version of the LDAP directory service is maintained on the Primary Directory Node (formerly referred to as master domain controller) and replicated to all the remaining LDAP servers of the UCS domain. As changes to the LDAP schema can occur during release updates, the Primary Directory Node must always be the first system to be updated during a release update.

2.2. UCS only available for 64 bit

Feedback 

UCS 5 is only provided for the x86 64 bit architecture (amd64). Existing 32 bit UCS systems cannot be updated to UCS 5.

Chapter 3. Simultaneous operation of UCS and Debian on UEFI systems

Please note that simultaneous operation of UCS and Debian on a UEFI system starting with UCS 5.0 is not supported.

The reason for this is the GRUB boot loader of Univention Corporate Server, which partly uses the same configuration files as Debian. An already installed Debian leads to the fact that UCS cannot be booted (any more) after the installation of or an update to UCS 5.0. A subsequent installation of Debian will also result in UCS 5.0 not being able to boot.

At the following help article further hints to this topic are collected: <https://help.univention.com/t/17768>

Chapter 4. Local package repository

This section is relevant for environments where a local repository is set up. The installed (major) version of UCS determines which packages a local repository provides. A repository running on a UCS server with version 4.x will only provide packages up to UCS 4.x, a repository server running on UCS 5 will only provide packages for UCS 5 and newer versions. To upgrade systems to UCS 5 in an environment with a local repository, the following are some of the options. First, a local UCS 5 repository server must be set up.

- A new UCS 5 system is installed as a Primary Directory Node from the DVD or from a virtualized base image. Then a local repository is set up on this system as described in the UCS 5 manual.
- A new UCS 5 system is installed with the system role Backup Directory Node, Replica Directory Node or Managed Node from the DVD or from a virtualized base image. In system setup, select that the system will not join a domain. Then set up a local repository on this system as described in the UCS 5 manual. After the Primary Directory Node used in the domain is upgraded to UCS 5, the UCS 5 repository server can join the domain via `univention-join`.

To upgrade a system in the domain to UCS 5, the server should first be upgraded to the latest package level available for UCS 4.x. Then the repository server used by the system is switched to the local UCS 5 repository by changing the Univention Configuration Registry variable `repository/online/server`. The system can now be upgraded to UCS 5 via the Univention Management Console or via the command line.

Chapter 5. Preparation of update

Manually crafted Python code needs to be checked for compatibility with Python 3.7 before the Update and adjusted accordingly. This includes Univention Configuration Registry templates containing Python code. Customized AD-Connector mapping templates are an example for this. See also the [developer-reference] for advice.

It must be checked whether sufficient disk space is available. A standard installation requires a minimum of 6-10 GB of disk space. The update requires approximately 1-2 GB additional disk space to download and install the packages, depending on the size of the existing installation.

For the update, a login should be performed on the system's local console as user `root`, and the update should be initiated there. Alternatively, the update can be conducted using Univention Management Console.

Remote updating via SSH is not recommended as this may result in the update procedure being canceled, e.g., if the network connection is interrupted. In consequence, this can affect the system severely. If updating should occur over a network connection nevertheless, it must be verified that the update continues in case of disconnection from the network. This can be achieved, e.g., using the tools `tmux`, `screen` and `at`. These tools are installed on all UCS system roles by default.

Univention provides a script that checks for problems which would prevent the successful update of the system. Prior to the update, this script can be downloaded and executed on the UCS system.

```
# download
curl -Oof https://updates.software-univention.de/download/univention-
update-checks/pre-update-checks-5.0-2{.gpg,}

# verify and run script
apt-key verify pre-update-checks-5.0-2{.gpg,} &&
  bash pre-update-checks-5.0-2

...

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
...
```


Chapter 6. Postprocessing of the update

Following the update, new or updated join scripts need to be executed. This can be done in two ways: Either using the UMC module **Domain join** or by running the command `univention-run-join-scripts` as user `root`.

Subsequently the UCS system needs to be restarted.

Chapter 7. Notes on selected packages

7.1. Collection of usage statistics


Feedback 

Anonymous usage statistics on the use of Univention Management Console are collected when using the *UCS Core Edition*. The modules opened get logged to an instance of the web traffic analysis tool Piwik. This makes it possible for Univention to tailor the development of Univention Management Console better to customer needs and carry out usability improvements.

This logging is only performed when the *UCS Core Edition* license is used. The license status can be verified via the menu entry **License** -> **License information** of the user menu in the upper right corner of Univention Management Console. If **UCS Core Edition** is listed under **License type**, this version is in use. When a regular UCS license is used, no usage statistics are collected.

Independent of the license used, the statistics generation can be deactivated by setting the Univention Configuration Registry variable `umc/web/piwik` to *false*.

7.2. Recommended browsers for the access to Univention Management Console

Feedback 

Univention Management Console uses numerous JavaScript and CSS functions to display the web interface. Cookies need to be permitted in the browser. The following browsers are recommended:


- Chrome as of version 85
- Firefox as of version 78
- Safari and Safari Mobile as of version 13
- Microsoft Edge as of version 88

Users running older browsers may experience display or performance issues.

Chapter 8. Changelog

Listed are the changes since UCS 5.0-1:

8.1. General


Feedback 

- Various unused Python 2 modules has been removed from the Debian packages (Bug 54706).
- The server password change mechanism has been adjusted to first validate that the new machine password successfully replicated in OpenLDAP before finally changing the password locally in Samba/AD. Quickly reverting password changes in AD easily breaks DRS replication, so prevent this situation from happening (Bug 53205).
- All security updates issued for UCS 5.0-1 are included:
 - *apache2* (CVE-2021-44224 CVE-2021-44790) (Bug 54298)
 - *bind9* (CVE-2021-25220) (Bug 54573)
 - *cifs-utils* (CVE-2022-27239 CVE-2022-29869) (Bug 54818)
 - *clamav* (CVE-2022-20698) (Bug 54599)
 - *cups* (CVE-2020-10001 CVE-2022-26691) (Bug 54598 Bug 54808)
 - *cyrus-sasl2* (CVE-2022-24407) (Bug 54490)
 - *dpkg* (Bug 54810)
 - *expat* (CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-23990 CVE-2022-25235 CVE-2022-25236 CVE-2022-25313 CVE-2022-25314 CVE-2022-25315) (Bug 54448 Bug 54480)
 - *firefox-esr* (CVE-2021-4140 CVE-2021-38503 CVE-2021-38504 CVE-2021-38506 CVE-2021-38507 CVE-2021-38508 CVE-2021-38509 CVE-2021-43534 CVE-2021-43535 CVE-2021-43536 CVE-2021-43537 CVE-2021-43538 CVE-2021-43539 CVE-2021-43541 CVE-2021-43542 CVE-2021-43543 CVE-2021-43545 CVE-2021-43546 CVE-2022-1097 CVE-2022-1196 CVE-2022-1529 CVE-2022-1802 CVE-2022-22737 CVE-2022-22738 CVE-2022-22739 CVE-2022-22740 CVE-2022-22741 CVE-2022-22742 CVE-2022-22743 CVE-2022-22745 CVE-2022-22747 CVE-2022-22748 CVE-2022-22751 CVE-2022-22754 CVE-2022-22756 CVE-2022-22759 CVE-2022-22760 CVE-2022-22761 CVE-2022-22763 CVE-2022-22764 CVE-2022-24713 CVE-2022-26381 CVE-2022-26383 CVE-2022-26384 CVE-2022-26386 CVE-2022-26387 CVE-2022-26485 CVE-2022-26486 CVE-2022-28281 CVE-2022-28282 CVE-2022-28285 CVE-2022-28286 CVE-2022-28289 CVE-2022-29909 CVE-2022-29911 CVE-2022-29912 CVE-2022-29914 CVE-2022-29916 CVE-2022-29917 CVE-2022-31736 CVE-2022-31737 CVE-2022-31738 CVE-2022-31740 CVE-2022-31741 CVE-2022-31742 CVE-2022-31747) (Bug 54345 Bug 54442 Bug 54512 Bug 54543 Bug 54654 Bug 54730 Bug 54787 Bug 54819)
 - *flac* (CVE-2020-0499) (Bug 54608)
 - *ghostscript* (Bug 54314)
 - *gmp* (CVE-2021-43618) (Bug 54602)

- **gzip** (CVE-2022-1271) (Bug 54672)
- **intel-microcode** (CVE-2021-0127 CVE-2021-0145 CVE-2021-33120) (Bug 54605)
- **jbig2dec** (CVE-2020-12268) (Bug 54610)
- **libpcap** (CVE-2019-15165) (Bug 54601)
- **libxml2** (CVE-2022-23308 CVE-2022-29824) (Bug 54609 Bug 54788)
- **linux, linux-latest, linux-signed-amd64** (CVE-2020-29374 CVE-2020-36322 CVE-2021-3640 CVE-2021-3744 CVE-2021-3752 CVE-2021-3760 CVE-2021-3764 CVE-2021-3772 CVE-2021-4002 CVE-2021-4083 CVE-2021-4135 CVE-2021-4149 CVE-2021-4155 CVE-2021-4202 CVE-2021-4203 CVE-2021-20317 CVE-2021-20321 CVE-2021-20322 CVE-2021-22600 CVE-2021-28711 CVE-2021-28712 CVE-2021-28713 CVE-2021-28714 CVE-2021-28715 CVE-2021-28950 CVE-2021-38300 CVE-2021-39685 CVE-2021-39686 CVE-2021-39698 CVE-2021-39713 CVE-2021-41864 CVE-2021-42739 CVE-2021-43389 CVE-2021-43975 CVE-2021-43976 CVE-2021-44733 CVE-2021-45095 CVE-2021-45469 CVE-2021-45480 CVE-2022-0001 CVE-2022-0002 CVE-2022-0322 CVE-2022-0330 CVE-2022-0435 CVE-2022-0487 CVE-2022-0492 CVE-2022-0617 CVE-2022-0644 CVE-2022-22942 CVE-2022-23036 CVE-2022-23037 CVE-2022-23038 CVE-2022-23039 CVE-2022-23040 CVE-2022-23041 CVE-2022-23042 CVE-2022-23960 CVE-2022-24448 CVE-2022-24958 CVE-2022-24959 CVE-2022-25258 CVE-2022-25375 CVE-2022-26966) (Bug 54541 Bug 54607)
- **lxml** (CVE-2021-43818) (Bug 54346)
- **mariadb-10.3** (CVE-2021-35604 CVE-2021-46659 CVE-2021-46661 CVE-2021-46662 CVE-2021-46663 CVE-2021-46664 CVE-2021-46665 CVE-2021-46667 CVE-2021-46668 CVE-2022-24048 CVE-2022-24050 CVE-2022-24051 CVE-2022-24052) (Bug 54604)
- **nbd** (CVE-2022-26495 CVE-2022-26496) (Bug 54542)
- **nss** (CVE-2022-22747) (Bug 54375)
- **ntfs-3g** (CVE-2021-46790 CVE-2022-30783 CVE-2022-30784 CVE-2022-30785 CVE-2022-30786 CVE-2022-30787 CVE-2022-30788 CVE-2022-30789) (Bug 54857)
- **openldap** (CVE-2022-29155) (Bug 54627 Bug 54783)
- **openssl** (CVE-2021-4160 CVE-2022-0778 CVE-2022-1292 CVE-CVE-2022-2068) (Bug 54557 Bug 54764 Bug 54901)
- **pillow** (CVE-2022-22815 CVE-2022-22816 CVE-2022-22817) (Bug 54366)
- **policykit-1** (CVE-2021-4034) (Bug 54374)
- **postgresql-11** (CVE-2022-1552) (Bug 54751)
- **rsyslog** (CVE-2019-17041 CVE-2019-17042 CVE-2022-24903) (Bug 54600 Bug 54809)
- **samba** (CVE-2021-43566 CVE-2021-44142 CVE-2022-0336) (Bug 53629 Bug 54015 Bug 54200 Bug 54278 Bug 54369)
- **squid** (CVE-2021-28116 CVE-2021-46784) (Bug 54907)


- *tiff* (CVE-2022-0561 CVE-2022-0562 CVE-2022-0865 CVE-2022-0891 CVE-2022-0907 CVE-2022-0908 CVE-2022-0909 CVE-2022-0924 CVE-2022-22844) (Bug 54595)
- *vim* (CVE-2019-20807 CVE-2021-3770 CVE-2021-3778 CVE-2021-3796) (Bug 54606)
- *xorg-server* (CVE-2021-4008 CVE-2021-4009 CVE-2021-4010 CVE-2021-4011) (Bug 54270)
- *xterm* (CVE-2022-24130) (Bug 54603)
- *xz-utils* (CVE-2022-1271) (Bug 54671)
- *zlib* (CVE-2018-25032) (Bug 54631)
- The following updated packages from Debian 10.12 are included (Bug 54866): *aide*, *apache-log4j1.2*, *apache-log4j2*, *atftp*, *base-files*, *beads*, *btrbk*, *cargo-mozilla*, *chrony*, *cimg*, *condor*, *debian-edu-config*, *debian-installer-netboot-images*, *debian-installer*, *detox*, *djvulibre*, *ecdsautils*, *evolution-data-server*, *exo*, *faad2*, *ffmpeg*, *firejail*, *gerbv*, *glibc*, *graphicsmagick*, *h2database*, *htmldoc*, *http-parser*, *icu*, *ipython*, *jtharness*, *jtreg*, *lemonldap-ng*, *leptonlib*, *libdatettime-timezone-perl*, *libencode-perl*, *libetpan*, *libextractor*, *libjackson-json-java*, *libmodbus*, *libphp-adodb*, *librecad*, *libsdl1.2*, *lighttpd*, *llvm-toolchain-11*, *lrzip*, *lxcfs*, *mailman*, *mediawiki*, *modsecurity-apache*, *needrestart*, *node-getobject*, *openjdk-11*, *openscad*, *opencs*, *php-illuminate-database*, *phpliteadmin*, *plib*, *privoxy*, *prosody*, *publicsuffix*, *python-bottle*, *python-virtualenv*, *raptor2*, *redis*, *ros-ros-comm*, *roundcube*, *ruby2.5*, *ruby-httpclient*, *rust-cbindgen*, *rustc-mozilla*, *smarty3*, *snappd*, *sogo*, *sphinxsearch*, *spip*, *strongswan*, *subversion*, *thunderbird*, *traf-ficsserver*, *tryton-proteus*, *tryton-server*, *tzdata*, *uriparser*, *usbview*, *varnish*, *vlc*, *waitress*, *wavpack*, *webkit2gtk*, *weechat*, *wireshark*, *wordpress*, *zsh*, *zziplib*
- The following packages have been moved to the maintained repository of UCS: *python-jose* (Bug 54666), *python-keycloak* (Bug 54689), *univention-support-info* (Bug 53358)

8.2. Univention Installer


 Feedback 

- Remove left-over static host configuration for 1.27.0.1.1 (Bug 49042).

8.3. Basic system services

 Feedback 

8.3.1. Univention Configuration Registry

 Feedback 


- Adapted the code due to a Linux kernel API change in v5.7-rc1~128, where `open(O_EXCL)` now returns `EEXIST` instead of `EISDIR` (Bug 54476).
- The remaining scripts have all been migrated to Python 3 (Bug 54208).
- The Python-API of Univention Configuration Registry has been extended to offer a method `get_int()`, that can be used to avoid receiving a string, when an integer is required. If the value of the requested Univention Configuration Registry variable is not a number, the default value is returned verbatim instead (Bug 20933).

8.3.1.1. Changes to templates and modules


 Feedback 

- The Univention Configuration Registry template for the file `/etc/hosts` now always produces the same output given the same configuration (Bug 54558).
- Clarified the description of the Univention Configuration Registry variable `logrotate/rotate/count` (Bug 54691).

8.4. Domain services


Feedback 

8.4.1. OpenLDAP

Feedback 


- The `ppolicy` overlay module uses embedded Python. This has been migrated to Python 3 (Bug 54582).
- The behavior of the `translog` overlay was modified to skip grandchildren of the `cn=temporary, cn=univention` container. This new behavior can be controlled by the Univention Configuration Registry variable `ldap/translog-ignore-temporary`. This reduces the number of replication transactions during creation of users and groups significantly. As a result it increases the replication performance and reduces the rate at which the `cn=translog` LMDB backend database gets filled. This variable is applicable only to the Primary Directory Node. The package *univention-ldap-server* activates this variable by default (Bug 48626).

8.4.1.1. Listener/Notifier domain replication

Feedback 


- An error when deactivating a listener module through UCR has been fixed (Bug 54696).
- `univention-translog import --min TID` had no effect (Bug 54794).
- Several memory issues have been fixed (Bug 49868).
- The Notifier sometimes failed to process all transaction in bulk and aborted. This lead to the Notifier making no progress and filling the log file with the same error messages again and again. Transactions are now processes incrementally (Bug 49868).
- If the number of transactions was lower than 1000, only a partial number of transactions has been imported during the join of a backup (Bug 54203).

8.4.2. DNS server

Feedback 


- The Univention Configuration Registry variable `dns/timeout-start` is now also considered in the `systemd` unit `univention-bind-ldap`. This can be used in cases where a large number of DNS zones slows down the start of the DNS server bind. This only affects systems which have `dns/backend` set to `ldap`. i.e. systems that are not configured as Samba/AD DC. After changing the variable, running `systemctl daemon-reload` once is required (Bug 54108).

8.4.3. Univention Directory Listener


Feedback 

- The unused method `get_configuration()` has been removed from the `ListenerModuleConfiguration` class in the `univention.listener.handler_configuration` module (Bug 54501).

8.5. Univention Management Console

Feedback 


8.5.1. Univention Management Console web interface

Feedback 

- A new widget suggesting mail domains while typing has been introduced (Bug 54467).
- The logic for mapping UDM syntax classes to UMC frontend widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug 38762).
- The domain component in an LDAP path is not shown in wrong reversed order anymore (Bug 53678).


- In case of a long-lasting login, certain UMC modules do not work properly. If this happens, a message will be displayed to the user containing a link to <https://help.univention.com/t/6413> (Bug 54032).
- A new method has been added to generate and set a service specific password for a user (Bug 54438).
- The UDM REST API now supports UDM object types containing – in their name (Bug 54063).
- The `entryUUID` and `dn` of newly created objects are now included in the response (Bug 54347).
- The UDM REST API now supports multiprocessing via the Univention Configuration Registry variable `directory/manager/rest/processes`. Further details can be found in the performance guide (Bug 50050).

8.5.2. Univention Portal

Feedback 


- The Portal server now fetches user information from the UMC server asynchronously (Bug 53853).
- Fixed various accessibility issues (Bug 54556).
- Fixed various CSS issues (Bug 54556).
- Added new tooltips. They comply with accessibility requirements (Bug 54556).
- Improved the translation widget when editing portal entries (Bug 54556).
- Fixed drag and drop behavior when using the keyboard, added screen reader support (Bug 54556).
- The portal now integrates the self service functionality: Reset passwords, change profile, verify accounts, etc is now possible from within the portal (Bug 54556).
- The French translation of UDM portal attributes has been updated (Bug 54029).
- Some requests have been excluded from `apache2/force_https`, so that the portal tiles in the UMC are shown even if https is forced (Bug 53296).
- The Portal server now provides a navigation endpoint (Bug 54618).
- Keywords can now be added to portal entries. They are not visible, but searchable (Bug 54295).
- Entries can now be opened in new tabs with a specific internal name ("target") (Bug 54633).

8.5.3. Univention Management Console server

Feedback 

- The function `DNSanitizer` has been added to the Python module variable `__all__` to prevent warnings for developers (Bug 52445).
- The cookie attribute `SameSite` can now be set for UMC cookies via the Univention Configuration Registry variable `umc/http/cookie/samesite` (Bug 54484).
- `univention-management-console-dev` now depends on both `imagemagick` and `inkscape` (Bug 54043).

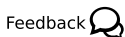
8.5.4. Univention App Center

Feedback 

- The reason why servers are excluded from the app-installation drop-down menu is displayed again (Bug 54460).

- Change order and prioritize App specific settings over App Center settings when populating the environment file. This is required for some upcoming Apps to be installed (Bug 54612).
- Allow for the `tmpfs` that are created for a docker app to be defined in the apps ini file (Bug 54562).
- A race condition was fixed, that caused apps to lose their installation status (Bug 54452).
- Validate the form when choosing the installation host (Bug 53523).
- Make the check regarding network conflicts with docker more robust (Bug 54082).


8.5.5. Univention Directory Manager UMC modules and command line interface



- The mapping of syntax class to UMC widgets via the Univention Configuration Registry variable `directory/manager/web/widget/. *` has been removed. This can now be achieved via syntax classes directly (Bug 54840).
- An error introduced in UCS 5.0-2 erratum 335 has been repaired which caused that e.g. the selection list of printer model in the printer shares module could not be fetched (Bug 54849).
- The error handling of the syntax class `jpegPhoto` was broken since UCS 5.0-0 and has been repaired (Bug 54769).
- Clarified error message for invalid host name or FQDN (Bug 54663).
- The available mail domains are now suggested when entering values for the attribute `mailPrimaryAddress` of objects `users/user` (Bug 54467).
- Syntax classes can now depend on another UDM property and restrict their choices based on that (Bug 53843).
- The logic for mapping UDM syntax classes to UMC frontend widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug 38762).
- A crash while accessing an user with multiple user certificates has been repaired (Bug 54617).
- Changing the case of the name or email attributes will no longer be prevented by the locking mechanism (Bug 52760).
- Some redundant log messages logging password hashes were removed (Bug 54348).
- The performance of the license check has been improved to reduce the initial login time (Bug 52292).
- Backend functionality for service specific passwords has been added. It cannot be used via CLI (Bug 54438).
- When removing a policy the policy is removed from the referencing objects (Bug 16966).
- Searching with patterns containing umlauts is possible again (Bug 53975).
- It is now possible to search for the user expiry date of `users/user` objects (Bug 54150).
- Two resource sharing conflicts on Python dictionaries have been fixed, that could lead to tracebacks when modules are reloaded in a multi-threaded context (Bug 53581).
- Moving of `users/ldap` objects is possible again. This was broken due to the Python 3 migration in UCS 5.0 (Bug 54085).


- When user templates were members of groups an error was raised which prevented opening or modifying that group. Templates as group members are now ignored in UDM module `groups/group` (Bug 54402).
- When setting an user as a member of a group in UDM, that had the same UID but a different DN of another member, the related attribute `memberUid` of the group got dropped. This happened in the cool Solution `user-group-sync`TM during move operations (Bug 54297).
- The French translation of UDM extended attributes has been updated (Bug 54029).
- The `entryUUID` of an LDAP object is now exposed by the UDM API (Bug 54883).

8.5.6. Modules for system settings / setup wizard

Feedback 


- The package `univention-system-setup` has been migrated to Python 3 (Bug 51318).

8.5.7. Domain join module

Feedback 


- When executing join scripts via UMC module `Domain Join` the progress bar will now display the name of the currently running script instead of the last script that was finished (Bug 33255).
- The joinscript of `univention-samba4` did pass the credentials in clear text to other tools like `ldbsearch` as command line arguments. To reduce the attack surface it now uses a file instead (Bug 53100).
- Joining a backup node into a single server UCS@school environment failed because the LDB module `univention_samaccountname_ldap_check` attempted to create an object of type `computers/windows` for it which always failed because the account name was already taken by the `computers/domaincontroller_backup` object (Bug 54768).
- Several memory and open file descriptor leaks have been fixed. An error restarting Samba during package installation has been fixed. The build system for the package has been cleaned up (Bug 48823).

8.5.8. Univention Directory Reports

Feedback 

- The script `univention-directory-reports` now offers two new options: The option `--output-dir` allows specification of the output directory and `--output-name` allows to specify the file name of the report (Bug 54153).


8.5.9. System diagnostic module

Feedback 

- A new diagnostic plugin has been added to detect cases where the group membership attributes `unique-Member` and `memberUid` are no longer consistent (Bug 48652).
- `52_mail_acl_sync` will no longer fail if multiple IMAP mail folders exist (Bug 54675).
- A new diagnostic plugin has been added to detect cases where an LDAP schema is missing that is actually still referenced by some objects (Bug 53455).
- The script `univention-run-diagnostic-check` now displays links in the description of failed tests (Bug 50756).
- Disk usage checks will now handle log level evaluations of Univention Configuration Registry variable `ldap/debug/level` correctly (Bug 49354).
- A diagnostic warning for the Samba replication status will now be formatted properly (Bug 53341).
- Mounted ISO images are no longer included in the disk usage diagnostic plugin (Bug 49353).


- The Python 3 compatibility when handling exceptions in certain diagnostic plugins has been corrected (Bug 53306).
- A diagnostic module has been added to check the Univention Configuration Registry variable `notifier/protocol/version` (Bug 54264).
- `univention-run-diagnostic-checks` now offers to run a group of tests and also to exclude some of the tests (Bug 53969).
- The script `univention-run-diagnostic-check` is now executed with machine account credentials by default (Bug 54515).
- The detection of `slapschema` error message has been improved in `62_check_slapschema` (Bug 54681).

8.5.10. Filesystem quota module

Feedback 


- Setting quotas for accounts with a fully numeric username has been fixed (Bug 54638).

8.5.11. Other modules

Feedback 


- Syntax classes can now depend on another UDM property and restrict their choices based on that (Bug 53843).
- The logic for mapping UDM syntax classes to UMC frontend widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug 38762).
- A UMC operation set enabling the creation of UDM Reports was added (Bug 54109).
- Byte values are now correctly decoded for the labels of choices delivered by the syntax class `LDAP_Search` (Bug 54190).
- The domain component in a LDAP path is not shown in wrong reversed order anymore (Bug 53678).
- The Univention Configuration Registry variable `directory/manager/web/modules/users/user/wizard/property/invite/default` will now work properly and can be used to activate the **invite user via e-mail** option in the user wizard by default (Bug 54316).

8.6. Univention base libraries

Feedback 


- Detecting UMC specific files did not work for packages having files, which have blanks in their filenames. This lead to error messages during package upgrades and inconsistent cache behavior (Bug 54047).
- `UCSVersion` not includes the erroneous input parameter is included in the error message for debugging (Bug 49061).
- Added the new function `generate_password` that can generate random passwords. The new function `password_config` can be used to get parameters for that from UCR (Bug 54555).
- Changing a user password is now possible again when the referenced password history policy did not define values for password length or history length (Bug 51354).
- For *Python-ldap-3.3.0* (and higher) some TLS settings are no longer immediately materialized. To ensure correct behavior of TLS encrypted LDAP connections, the option `OPT_X_TLS_NEWCTX` will be necessary for future UCS versions (Bug 54408).

8.7. Software deployment


 Feedback 

- `univention-upgrade --update` is parsed earlier and exits on wrong parameter (Bug 49061).
- `apt-get --force-yes` option is deprecated and has been replaced with `--allow-unauthenticated --allow-downgrades --allow-remove-essential --allow-change-held-packages` (Bug 48891).
- App updates invoked by `univention-upgrade` will now work correctly (Bug 53666).

8.8. System services


 Feedback 

8.8.1. PostgreSQL

 Feedback 


- During the upgrade to UCS 5.0-1 PostgreSQL 11 might have been disabled by setting the Univention Configuration Registry variable `postgres11/autostart=no` by accident (Bug 54255).

8.8.2. Docker

 Feedback 


- The script `migrate_container_MountPoints_to_v2_config` is deprecated since UCS 4.3 and has been removed (Bug 52539).
- The package `univention-docker-container-mode` is deprecated since UCS 4.3 and has been replaced by an empty transitional package (Bug 52539).

8.8.3. SAML

 Feedback 

- The cookie attributes `Secure` and `SameSite` can now be set for the session and language cookies of SAML Identity Providers via Univention Configuration Registry variable `saml/idp/session-cookie/secure`, `saml/idp/session-cookie/samesite`, `saml/idp/language-cookie/secure` and `saml/idp/language-cookie/samesite` (Bug 54483).
- The link to the self service has been changed to point to the new portal based self service (Bug 54556).
- An internal ID has been fixed, which caused the German translation not being shown when new passwords did not match (Bug 54268).
- The French translation of UDM extended attributes has been updated (Bug 54029).


8.8.4. Univention self service

 Feedback 

- The logic for mapping UDM syntax classes to UMC frontend widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug 38762).
- The Self Service now adds its dedicated portal to make use of the new features in Univention Portal. For more, see <https://help.univention.com/t/19671> (Bug 54556).
- A new backend function has been added that can set service specific passwords for a user (Bug 54434).
- The e-mail template for password reset tokens now support additional placeholders for the properties `title`, `initials`, `displayName`, `firstname`, `lastname`, `mailPrimaryAddress`, `employeeNumber` and `organisation` (Bug 48960).
- The package has been migrated to Python 3. Custom plugins for sending the password recovery tokens also need to be migrated to Python 3 (Bug 51327 Bug 54466).


- The French translation of UDM extended attributes and portal attributes has been updated (Bug 54029).

8.8.5. Mail services

Feedback 


- The French translation of UDM extended attributes has been updated (Bug 54029).
- A bug where antivirus signatures could not get updated properly on fresh installations has been fixed (Bug 54070).

8.8.6. Dovecot

Feedback 


- The French translation of UDM extended attributes has been updated (Bug 54029).

8.8.7. Postfix

Feedback 


- Error handling in the script `/usr/share/univention-mail-postfix/listfilter.py` has been repaired (Bug 54560).

8.8.8. Monitoring / Nagios

Feedback 


- A new monitoring system has been implemented based on Prometheus, Prometheus Alertmanager and Grafana. During the upgrade all current Nagios services are migrated to Monitoring alerts (Bug 54748, Bug 54749, Bug 54750).
- The configuration of NRPE plugin definitions was broken due to the migration to Python 3 and has been repaired (Bug 53681).
- The Nagios plugins in *univention-nagios-client* have been converted to Python 3 (Bug 52258).

8.8.9. Apache

Feedback 


- Apache can now be configured to only support TLS v1.3 connections by setting the Univention Configuration Registry variable `ucr set apache2/ssl/tlsv13=true` (Bug 54306).

8.8.10. RADIUS

Feedback 


- The RADIUS server can now assign VLAN IDs to user connections if their group has set the attribute `vlanId`. The Univention Configuration Registry variable `freeradius/vlan-id` has been added to set a VLAN ID even if the user is no member of any such group (Bug 25916).
- A new Univention Configuration Registry variable `radius/use-service-specific-passwords` has been added: If enabled, the authentication is done against a RADIUS specific password, not the domain password of the user (Bug 54409).
- An error while adding the French translation to an extended attribute during the package update has been fixed (Bug 54461).
- The French translation of UDM extended attributes has been updated (Bug 54029).
- Updating an old RADIUS installation will now correctly update the description for the extended attributes `networkAccessGroups` and `NetworkAccessComputers` (Bug 54341).

8.8.11. Proxy services

Feedback 

- The package *univention-squid* has been migrated to Python 3 (Bug 53357).

8.8.12. Kerberos

Feedback 


- The Kerberos ticket lifetime was made configurable via Univention Configuration Registry variable `kerberos/defaults/ticket-lifetime` (Bug 52987).

8.8.13. SSL

Feedback 

- Some web browsers refused wildcard certificates generated by `univention-certificates` because the information was only stored in *common name* but required in *subject alternative names*, too (Bug 53288).

8.8.14. DHCP server


Feedback 

- Add UCR packages to profile for network installation (Bug 54259).

8.9. Services for Windows

Feedback 

8.9.1. Samba

Feedback 

- Samba has been updated to version 4.16.2 (Bug 54682).
- In some cases, in UCS@school the `log.smbd` filled with a message because a Windows 10 client attempted to access user files, which is denied by the NTACLs. While the origin of that behavior is still unknown, no negative side effects are known. To avoid overflowing the log file, we adjusted the log message to only start appearing at the debug level 2. Default log level is 1 (Bug 52979).
- `samba-tool` now supports passing credentials using the option `--authentication-file` and the machine password using the option `--machinepass-file` (Bug 53101).
- The share configuration of *vfs objects*, *write list*, *hosts allow* and *hosts deny* was broken because of too excessive escaping of quotes and has been repaired (Bug 49842).
- The share setting `map acl inherit = yes` has been broken since UCS 5.0-0 and is not working properly again (Bug 54688).
- The access to home shares via NTLM authentication on member server has been fixed (Bug 54200).
- The joinscript of `univention-samba4` did pass the credentials in clear text to other tools like `ldbsearch` as command line arguments. To reduce the attack surface it now uses a file instead (Bug 53100).
- During a server password change the Samba process was not restarted in some cases. The script to restart Samba was fixed to ensure the service is restarted successfully (Bug 54356).
- The Kerberos ticket lifetime was made configurable via Univention Configuration Registry variable `kerberos/defaults/ticket-lifetime` (Bug 52987).


8.9.2. Univention AD Takeover

Feedback 

- `samba-tool` now supports passing machine password using the option `--machinepass-file` (Bug 53101).
- `samba-tool` now supports passing credentials using the options `-A|--authentication-file` (Bug 53101).
- Performing an Active Directory takeover will work when the original AD contains Group Policy Objects that use non ASCII encoding (Bug 54196).


- Invalid (empty) UCR network interface configuration lead to network failure during AD Takeover (Bug 54359).
- On systems updated from UCS 4.4 the AD-Takeover could abort with a traceback because the `systemctl` command was not found under the path specified in the Python code (Bug 54238).

8.9.3. Univention S4 Connector

Feedback 


- The user expiry was off by one day between UCS and Samba. This discrepancy has been removed (Bug 53012).

8.9.4. Univention Active Directory Connection

Feedback 

- For *Python-ldap-3.3.0* (and higher) some TLS settings are no longer immediately materialized. To ensure correct behavior of TLS encrypted LDAP connections, the option `OPT_X_TLS_NEWCTX` will be necessary for future UCS versions (Bug 54408).

8.10. Other changes

Feedback 

- Improve message consistency between the man page and the `--help` messages (Bug 54588).
- Fix spelling mistake of `rsync` in `doc/univention-ssh.8` (Bug 54588).
- Update the `univention-scp --help` and `univention-rsync` message to specify that the `--no-split` option must be set before the password file parameter (Bug 54588).
- Added support for RFC6265bis *SameSite* cookie attribute (Bug 54483).
- Fixed Python 2 compatibility of UCR template `slapd.conf.d/65admingrp-user-password-reset` introduced by UCS 5.0-2 erratum 308 (Bug 54790).
- The start of OpenLDAP could fail if the ACL lines got too long. This could happen if the Univention Configuration Registry variable `ldap/acl/user/passwordreset/.*` have a lot of values (Bug 54744).
- The group membership cache now returns an empty list instead of `None` when requesting non-existing keys. This fixes a traceback in the Microsoft 365 connector listener, when not every *ADConnectionAlias* has at least one user (Bug 54572).
- The French translation of UDM extended attributes has been updated (Bug 54029).
- A new attribute *univentionRadiusPassword* has been added to the user class (Bug 54395).
- The French translation of UDM extended attributes has been updated (Bug 54029).
- A new Univention Configuration Registry variable `ldap/translog-ignore-temporary` has been created to control if UDM temporary objects should be considered for replication by the OpenLDAP `translog` overlay which feeds the Listener/Notifier. This reduces the number of replication transactions during creation of users and groups significantly. As a result it increases the replication performance and reduces the rate at which the `cn=translog` LMDB backend database gets filled. This variable is applicable only to the Primary Directory Node. By default it will be set to `yes` during package installation and update (Bug 48626).
- A new LDAP attribute has been introduced with UCS 5.0-2 erratum 100. As re-indexing is time consuming the decision was made to delay the indexing until 5.0-2 and not to do it via an errata update. Therefore, a manual fix for customers is available and the required steps are documented at <http://help.univention.com/t/19248> (Bug 54092).

Other changes

- The French translation package has been given a comprehensive update to align it to the current source code. All missing translation strings have been added and all outdated ones updated along with some general improvements of existing translation strings (Bug 54029).
- Bugs in the localization template files were updated to fix the creation and update process of language packages (Bug 54029).

Bibliography

[ucs-performance-guide] Univention GmbH. 2021. *UCS performance guide*. <https://docs.software-univention.de/performance-guide-5.0.html>.

[developer-reference] Univention GmbH. 2021. *Univention Developer Reference*. <https://docs.software-univention.de/developer-reference-5.0.html>.