



# **Changelog for Univention Corporate Server (UCS) 5.2-0**

*Release 5.2-0*

**Jan 29, 2025**

The source of this document is licensed under GNU Affero General Public License v3.0 only.

# CONTENTS

<b>1</b>	<b>General</b>	<b>1</b>
<b>2</b>	<b>Basic system services</b>	<b>3</b>
2.1	Univention Configuration Registry . . . . .	3
2.2	Other system services . . . . .	3
<b>3</b>	<b>Domain services</b>	<b>5</b>
3.1	OpenLDAP . . . . .	5
3.2	DNS server . . . . .	5
3.3	LDAP Directory Manager . . . . .	5
3.4	Keycloak . . . . .	6
<b>4</b>	<b>Univention Management Console</b>	<b>7</b>
4.1	Univention Portal . . . . .	7
4.2	Univention App Center . . . . .	7
4.3	User management . . . . .	7
4.4	System diagnostic module . . . . .	7
<b>5</b>	<b>Univention base libraries</b>	<b>9</b>
<b>6</b>	<b>Software deployment</b>	<b>11</b>
<b>7</b>	<b>System services</b>	<b>13</b>
7.1	PostgreSQL . . . . .	13
7.2	Mail services . . . . .	13
7.3	Printing services . . . . .	13
7.4	Nagios . . . . .	13
7.5	RADIUS . . . . .	14
7.6	SSL/TLS . . . . .	14
7.7	DHCP services . . . . .	14
7.8	PAM / Local group cache . . . . .	14
7.9	NFS . . . . .	15
7.10	NTP . . . . .	15
<b>8</b>	<b>Services for Windows</b>	<b>17</b>
8.1	Samba . . . . .	17
	<b>Index</b>	<b>19</b>



**GENERAL**

- The version of all modified join scripts has been increased by 10 so that join script versions in UCS 5.0-x can be increased after UCS 5.1 has been released (Bug #56927).
- All Python 2.7 packages have been removed (Bug #56533, Bug #56533, Bug #55994).
- The code compatibility for Python 3.11 has been improved (Bug #55915).
- The package management library of **univention-lib** has been adjusted to upstream changes in **apt** (Bug #56536).
- Code which ensured compatibility with Python 2.7 has been removed (Bug #56604).
- Various dependencies on old transitional Debian and Univention packages have been replaced with dependencies on new successor packages. The **univention-saml** packages were transitional since UCS 5.1 and have now been removed completely (Bug #56858).
- The argument to the `--ucsversionstart` flag for `ucs_registerLDAPExtension` has been changed to `5.0-7` (Bug #56124).



## BASIC SYSTEM SERVICES

### 2.1 Univention Configuration Registry

- Strict type checking has been enabled when setting or modifying Univention Configuration Registry Variables (Bug #55981).

#### 2.1.1 Changes to templates and modules

- The deprecated SSH configuration option `ChallengeResponseAuthentication` has been replaced with `KbdInteractiveAuthentication`. The new Univention Configuration Registry Variable `sshd/KbdInteractiveAuthentication` allows to configure this option (Bug #56147).
- Scripts have been adjusted for binary paths changed in Debian (Bug #56665).
- Various Univention Configuration Registry templates have been updated to closer match upstream Debian 12 configuration. The Univention Configuration Registry Variable `syslog/template/default` has been deleted. The template files `/etc/default/samba` and `/etc/default/apache2` have been deleted (Bug #46120).
- The package `ntp` has been replaced by the package `ntpsec` (Bug #56661).

### 2.2 Other system services

- `univention-ssh` has been adjusted to work with `openssh-8.4-p1` (Bug #56593).





## DOMAIN SERVICES

### 3.1 OpenLDAP

- The configurability of the LDAP overlay module `memberOf` has been removed. Since UCS 4.3, UCS needs the `memberOf` overlay and activates it by default (Bug #56662).
- All LDAP utility command line calls have been adjusted to use `-H LDAP_URI` instead of the obsolete `-h host -p port` arguments (Bug #55997).
- Support for the **Berkeley DB** database backend for **OpenLDAP** has been removed (Bug #57112).
- The Univention Virtual Machine Manager related LDAP schema and objects are automatically removed during the upgrade to UCS 5.2 (Bug #56651).

#### 3.1.1 LDAP schema changes

- The LDAP attributes `univentionFetchmailAddress`, `univentionFetchmailServer`, `univentionFetchmailProtocol`, `univentionFetchmailPasswd`, `univentionFetchmailKeepMailOnServer` and `univentionFetchmailUseSSL` are deprecated, `univentionFetchmailSingle` is used instead for Fetchmail configurations (Bug #55905).

#### 3.1.2 Listener/Notifier domain replication

- Listener modules are now executed with Python 3.11 (Bug #56533).

### 3.2 DNS server

- All **systemd** references for the renamed `named.service` have been adjusted (Bug #56003).

### 3.3 LDAP Directory Manager

- The HTTP status code for move operations has been fixed to 202 for *ACCEPTED* (Bug #55057).
- The obsolete UDM modules `settings/portal*` have been removed (Bug #52048).
- The list of country names for the UDM syntax class `Country` has been updated (Bug #56541).
- Moving of objects without children is now done directly and doesn't require a HTTP redirection (Bug #55019).
- A migration of the LDAP data for the mapping of the UDM property `country` to the LDAP attribute `c` is now enforced for the upgrade to UCS 5.2 (Bug #56528).

- The default values of Univention Configuration Registry Variable `directory/manager/user/enable-legacy-username-format` and Univention Configuration Registry Variable `directory/manager/group/enable-legacy-cn-format` have been changed to `false` which configures UCS to disallow purely numerical user and group names (Bug #56992).
- The Univention Configuration Registry Variable `directory/manager/user/group-memberships-via-memberof` has been removed. Group memberships in the UDM module `users/user` are now always resolved through the LDAP attribute `memberOf` (Bug #56253).

### 3.4 Keycloak

- Several changes to `univention-keycloak` for better integration with Univention Nubus (Bug #57492).
- Starting with UCS 5.2-0, the Identity Provider (IDP) endpoint for SAML and OIDC services for all UCS systems is defined by the policy `sso_uri_domainwide_setting`. This policy sets the Univention Configuration Registry Variable `ucs/server/sso/uri` on all UCS systems in the domain. During installation of the **Keycloak** app or when changing the FQDN of the IDP, this policy is automatically updated. Services can use the value of `ucs/server/sso/uri` to configure SSO (Single Sign-on) with **Keycloak** on systems with at least UCS 5.2-0 (Bug #57826).

## UNIVENTION MANAGEMENT CONSOLE

- Deprecated Python APIs especially regarding the use of `python-notifier` have been removed (Bug #56538).

### 4.1 Univention Portal

- The UCS Portal's graphical user interface has received various updates (Bug #57083).

### 4.2 Univention App Center

- Removed the commands `univention-rename-app` and `univention-register-apps` which used old code that didn't work since at least UCS 5.0 and which are unneeded (Bug #56724).
- The initial App Center cache has been updated. It's important especially when working offline (Bug #56716).
- Adapted code to API changes in the new Python `apt` library (Bug #56598).
- The Docker daemon is configured to log to `journald` by default now, not in per-container JSON log files. `journald` can be queried to get the logs for one app (Bug #56058, Bug #56131).
- The obsolete Univention Configuration Registry Variable `docker/daemon/default/map/. *` has been removed from the Docker configuration templates and is no longer evaluated (Bug #56058).
- The App Center now avoids assigning a subnet to an app that conflicts with other networks already created in Docker (Bug #57210).

### 4.3 User management

- The deprecated self service frontend `/univention/self-service/` that came with UCS 4.4 has been removed (Bug #56601). Since UCS 5.0, the self service frontend is `/univention/selfservice/`.

### 4.4 System diagnostic module

- The diagnostic script `62_check_slapschema` has been adjusted to changed output of `slapschema` (Bug #56546).
- Added diagnostic script `68_old_fetchmail_attributes` to detect the use of deprecated Fetchmail LDAP attributes (Bug #55905).



## UNIVENTON BASE LIBRARIES

- The package dependencies have been adjusted to depend on **libldap-2.5-0** ([Bug #56596](#)).
- The concept `decode_ignorelist` has been removed. UDM doesn't decode attributes automatically anymore since UCS 5.0 ([Bug #50343](#)).



## SOFTWARE DEPLOYMENT

- During the update to UCS 5.2, objects from deprecated UCS versions are deleted from the LDAP directory. Information about deleted objects and the objects LDIF output can be found in the log file `/var/univention-backup/update-to-5.2-0/removed_with_ucs5_<timestamp>.ldif` (Bug #56134).





## SYSTEM SERVICES

### 7.1 PostgreSQL

- PostgreSQL has been upgraded to version 15. As administrator, you now have the option to change the password encryption to `scram-sha-256`. This can be achieved by using the UCR variables Univention Configuration Registry Variable `postgres15/password-encryption` and Univention Configuration Registry Variable `postgres15/pg_hba/password-encryption` (Bug #56540).

### 7.2 Mail services

- Some deprecated Fetchmail LDAP attributes are now hidden in UMC. Their data is automatically migrated during upgrade (Bug #55905).

#### 7.2.1 IMAP services

- The Univention Configuration Registry Variable `mail/dovecot/ssl/protocols` has been replaced with Univention Configuration Registry Variable `mail/dovecot/ssl/min_protocol` and must manually be set. The minimum required TLS version has been adjusted to TLS 1.2. The TLS versions 1.0 and 1.1 are no longer supported with default settings (Bug #56544).

### 7.3 Printing services

- The printer driver list has been updated (Bug #56542).

### 7.4 Nagios

- The Nagios server functionality has been removed from UDM. Therefore, the UDM module `nagios/timeperiod` has been removed. The UDM module `nagios/service` has been reduced to the minimal required NRPE properties (Bug #56367).
- LDAP credentials are now passed through the environment variable `LDAP_PASSWORD` instead of using the deprecated option `-y` (Bug #56580).
- The patches to **monitoring-plugins** have been adapted to the new upstream version. The patch adding the option `-y` to read the LDAP credentials from a file has been dropped. The patch fixing a spelling mistake has been dropped as it has been fixed upstream (Bug #55829).

## 7.5 RADIUS

- FreeRADIUS now uses TLS 1.3 as default maximum TLS version. TLS 1.3 may cause issues for Microsoft Windows 10 Clients. See UCS Manual (Bug #55763).
- The MD4 functionality is now provided by the `python3-samba` package, because it was dropped from OpenSSL (Bug #55996).
- The FreeRADIUS service now uses a specific credentials file in `/etc/freeradius.secret` (Bug #55963).

## 7.6 SSL/TLS

- Radius now has TLS 1.3 enabled by default. TLS 1.3 might cause issues with Microsoft Windows 10. To use TLS 1.2, set the Univention Configuration Registry Variable `freeradius/conf/tls-max-version` to the value `1.2` (Bug #55763).

## 7.7 DHCP services

- The LDAP configuration in `dhcpcd.conf` has been turned off temporarily during UCS 5.1 to avoid issues with `isc-dhcp-server` version `4.4.1-2.3` running into a thread deadlock when testing the configuration (Bug #56730).

## 7.8 PAM / Local group cache

- The deprecated `libnss-ldap` and `libpam-ldap` have been replaced with `sssd`. `sssd` is currently used for users only. This also means that `nscd` isn't used any longer for the `passwd` related system calls, but it still is used as cache for `hosts` resolution. The UCR variables `nscd/passwd/.` aren't used any longer.

The `sssd` is configured through `/etc/sss/sss.conf` which is generated from a UCR template now. `sssd` additionally reads configuration sub files from the directory `/etc/sss/conf.d` which can be used in case options need to be customized differently from what the UCR template initially supports.

The user cache of `sssd` can be flushed by running `sss_cache -U`, instead of running `nscd -i passwd`.

Note that `sssd` by default doesn't dynamically enumerate accounts in `passwd`. Some tools that expect that by default, may need adjustment to consider this. For example, `repquota` needs to be called with the option `-C` to resolve `uid` numbers to names.

Additionally, `sssd` doesn't support resolving shadow information at all, so for example `pam_unix` won't be able to read shadow related information for domain users. There's a difference between domain users managed in UDM/LDAP and traditional Linux local accounts.

Also note that UCS currently still uses `pam_krb5` separately from `sssd`, as UCS and Samba use *Heimdal Kerberos*, while `sssd` may be more leaning towards *MIT Kerberos* (Bug #56793).

- The obsolete `pam-tally` has been replaced with `pam-faillock` (Bug #56547).
- The obsolete `libpam-cracklib` has been replaced with `libpam-pwquality` (Bug #56002).
- The `pam` configuration file `/etc/pam.d/common-session-noninteractive` is now generated from a UCR template (Bug #57298).

## 7.9 NFS

- The **systemd** service unit for **nfs-kernel-server** has been adjusted to make restarts possible again (Bug #56545).

## 7.10 NTP

- The **ntpsec** service has been updated to version 1.2.3 to support MS-SNTP (Bug #57147).



## SERVICES FOR WINDOWS

### 8.1 Samba

- **samba** has been updated to version 4.21.1 (Bug #57690).
- The default for the Samba database is now `mdb` (Bug #57145).
- **samba-tool** has been adjusted to revert the changes for Samba Bug 14676 which caused a regression for `samba-tool` backup with `mdb` backend database (Bug #57297).



## INDEX

### B

#### Bugzilla

Bug #46120, 3  
Bug #50343, 9  
Bug #52048, 5  
Bug #55019, 5  
Bug #55057, 5  
Bug #55763, 14  
Bug #55829, 13  
Bug #55905, 5, 7, 13  
Bug #55915, 1  
Bug #55963, 14  
Bug #55981, 3  
Bug #55994, 1  
Bug #55996, 14  
Bug #55997, 5  
Bug #56002, 14  
Bug #56003, 5  
Bug #56058, 7  
Bug #56124, 1  
Bug #56131, 7  
Bug #56134, 11  
Bug #56147, 3  
Bug #56253, 6  
Bug #56367, 13  
Bug #56528, 5  
Bug #56533, 1, 5  
Bug #56536, 1  
Bug #56538, 7  
Bug #56540, 13  
Bug #56541, 5  
Bug #56542, 13  
Bug #56544, 13  
Bug #56545, 15  
Bug #56546, 7  
Bug #56547, 14  
Bug #56580, 13  
Bug #56593, 3  
Bug #56596, 9  
Bug #56598, 7  
Bug #56601, 7  
Bug #56604, 1  
Bug #56651, 5  
Bug #56661, 3  
Bug #56662, 5  
Bug #56665, 3

Bug #56716, 7  
Bug #56724, 7  
Bug #56730, 14  
Bug #56793, 14  
Bug #56858, 1  
Bug #56927, 1  
Bug #56992, 6  
Bug #57083, 7  
Bug #57112, 5  
Bug #57145, 17  
Bug #57147, 15  
Bug #57210, 7  
Bug #57297, 17  
Bug #57298, 14  
Bug #57492, 6  
Bug #57690, 17  
Bug #57826, 6

### D

directory/manager/group/enable-legacy-cn-format,  
6  
directory/manager/user/enable-legacy-username-format,  
6  
directory/manager/user/group-memberships-via-memberof,  
6  
docker/daemon/default/map/.\*, 7

### E

environment variable  
  directory/manager/group/enable-legacy-cn-format,  
  6  
  directory/manager/user/enable-legacy-username-format,  
  6  
  directory/manager/user/group-memberships-via-memberof,  
  6  
docker/daemon/default/map/.\*, 7  
freeradius/conf/tls-max-version, 14  
LDAP\_PASSWORD, 13  
mail/dovecot/ssl/min\_protocol, 13  
mail/dovecot/ssl/protocols, 13  
nscd/passwd/., 14  
postgres15/password-encryption, 13

postgres15/pg\_hba/password-encryption,  
13  
sshd/KbdInteractiveAuthentication,  
3  
syslog/template/default, 3  
ucs/server/sso/uri, 6

## F

freeradius/conf/tls-max-version, 14

## L

LDAP\_PASSWORD, 13

## M

mail/dovecot/ssl/min\_protocol, 13  
mail/dovecot/ssl/protocols, 13

## N

nscd/passwd/., 14

## P

postgres15/password-encryption, 13  
postgres15/pg\_hba/password-encryption,  
13

## S

sshd/KbdInteractiveAuthentication, 3  
syslog/template/default, 3

## U

ucs/server/sso/uri, 6