univention
be open.

Changelog for Univention Corporate Server (UCS) 5.0-9

Release 5.0-9

Sep 24, 2024

CONTENTS

CHAPTER

ONE

GENERAL

- UCS 5.0-9 includes all issued security updates issued for UCS 5.0-8:
  - **aom** (CVE-2024-5171) (Bug #57497)
  - **apache2** (CVE-2024-36387, CVE-2024-38476, CVE-2024-38477, CVE-2024-38573, CVE-2024-39884, CVE-2024-40725) (Bug #57554)
  - **bind9** (CVE-2023-4408, CVE-2024-1737, CVE-2024-1975) (Bug #57558)
  - **binutils** (CVE-2018-1000876, CVE-2018-12934) (Bug #57462)
  - **bluez** (CVE-2023-50229, CVE-2023-50230) (Bug #57571)
  - **cups** (CVE-2024-35235) (Bug #57382)
  - **curl** (CVE-2024-7264) (Bug #57503)
  - **dovecot** (CVE-2024-23184, CVE-2024-23185) (Bug #57570)
  - **emacs** (CVE-2024-39331) (Bug #57416)
  - **exim4** (CVE-2024-39929) (Bug #57496)
  - **firefox-esr** (CVE-2024-5688, CVE-2024-5690, CVE-2024-5691, CVE-2024-5693, CVE-2024-5696, CVE-2024-5700, CVE-2024-5702) (Bug #57385)
  - **gdk-pixbuf** (CVE-2022-48622) (Bug #57523)
  - **git** (CVE-2019-1387, CVE-2023-25652, CVE-2023-25815, CVE-2023-29007, CVE-2024-32002, CVE-2024-32004, CVE-2024-32021, CVE-2024-32465) (Bug #57412)
  - **glibc** (CVE-2024-33599, CVE-2024-33600, CVE-2024-33601, CVE-2024-33602) (Bug #57415)
  - **imagemagick** (CVE-2023-1289, CVE-2023-34151) (Bug #57461, Bug #57478)
  - **intel-microcode** (CVE-2023-42667, CVE-2023-45733, CVE-2023-45745, CVE-2023-46103, CVE-2023-47855, CVE-2023-49141, CVE-2024-24853, CVE-2024-24980, CVE-2024-25939) (Bug #57557)
  - **krb5** (CVE-2024-26458, CVE-2024-26461, CVE-2024-37370, CVE-2024-37371) (Bug #57476)
  - **libvpx** (CVE-2024-5197) (Bug #57387)
  - **libxml2** (CVE-2016-3709, CVE-2022-2309) (Bug #57573)
  - **linux** (CVE-2021-33630, CVE-2022-48627, CVE-2023-0386, CVE-2023-46838, CVE-2023-47233, CVE-2023-52340, CVE-2023-52429, CVE-2023-52436, CVE-2023-52439, CVE-2023-52443, CVE-2023-52444, CVE-2023-52445, CVE-2023-52449, CVE-2023-52464, CVE-2023-52469, CVE-2023-52470, CVE-2023-52486, CVE-2023-52583, CVE-2023-52587, CVE-2023-52594, CVE-2023-52599, CVE-2023-52600, CVE-2023-52601, CVE-2023-52602, CVE-2023-52603, CVE-2023-52604, CVE-2023-52609, CVE-2023-52612, CVE-2023-52615, CVE-2023-52619, CVE-2023-52620, CVE-2023-52622, CVE-2023-52623, CVE-2023-52628, CVE-2023-52644, CVE-2023-52650, CVE-2023-52670, CVE-2023-52679, CVE-2023-52683, CVE-2023-52691, CVE-2023-52693, CVE-2023-52698, CVE-2023-52699, CVE-2023-52880, CVE-2023-6040, CVE-2023-6270, CVE-2023-7042, CVE-2024-0340, CVE-2024-0607,

CVE-2024-1086, CVE-2024-22099, CVE-2024-23849, CVE-2024-24857, CVE-2024-24858, CVE-2024-24861, CVE-2024-25739, CVE-2024-26597, CVE-2024-26600, CVE-2024-26602, CVE-2024-26606, CVE-2024-26615, CVE-2024-26625, CVE-2024-26633, CVE-2024-26635, CVE-2024-26636, CVE-2024-26642, CVE-2024-26645, CVE-2024-26651, CVE-2024-26663, CVE-2024-26664, CVE-2024-26671, CVE-2024-26675, CVE-2024-26679, CVE-2024-26685, CVE-2024-26696, CVE-2024-26697, CVE-2024-26704, CVE-2024-26720, CVE-2024-26722, CVE-2024-26735, CVE-2024-26744, CVE-2024-26752, CVE-2024-26754, CVE-2024-26763, CVE-2024-26764, CVE-2024-26766, CVE-2024-26772, CVE-2024-26773, CVE-2024-26777, CVE-2024-26778, CVE-2024-26779, CVE-2024-26791, CVE-2024-26793, CVE-2024-26801, CVE-2024-26805, CVE-2024-26816, CVE-2024-26817, CVE-2024-26820, CVE-2024-26825, CVE-2024-26839, CVE-2024-26840, CVE-2024-26845, CVE-2024-26851, CVE-2024-26852, CVE-2024-26857, CVE-2024-26859, CVE-2024-26863, CVE-2024-26874, CVE-2024-26875, CVE-2024-26878, CVE-2024-26880, CVE-2024-26883, CVE-2024-26884, CVE-2024-26889, CVE-2024-26894, CVE-2024-26901, CVE-2024-26903, CVE-2024-26917, CVE-2024-26922, CVE-2024-26923, CVE-2024-26931, CVE-2024-26934, CVE-2024-26955, CVE-2024-26956, CVE-2024-26965, CVE-2024-26966, CVE-2024-26969, CVE-2024-26973, CVE-2024-26974, CVE-2024-26976, CVE-2024-26981, CVE-2024-26984, CVE-2024-26993, CVE-2024-26994, CVE-2024-26997, CVE-2024-27001, CVE-2024-27008, CVE-2024-27013, CVE-2024-27020, CVE-2024-27024, CVE-2024-27028, CVE-2024-27043, CVE-2024-27046, CVE-2024-27059, CVE-2024-27074, CVE-2024-27075, CVE-2024-27077, CVE-2024-27078, CVE-2024-27388, CVE-2024-27395, CVE-2024-27396, CVE-2024-27398, CVE-2024-27399, CVE-2024-27401, CVE-2024-27405, CVE-2024-27410, CVE-2024-27412, CVE-2024-27413, CVE-2024-27416, CVE-2024-27419, CVE-2024-27436, CVE-2024-31076, CVE-2024-33621, CVE-2024-35789, CVE-2024-35806, CVE-2024-35807, CVE-2024-35809, CVE-2024-35815, CVE-2024-35819, CVE-2024-35821, CVE-2024-35822, CVE-2024-35823, CVE-2024-35825, CVE-2024-35828, CVE-2024-35830, CVE-2024-35835, CVE-2024-35847, CVE-2024-35849, CVE-2024-35877, CVE-2024-35886, CVE-2024-35888, CVE-2024-35893, CVE-2024-35898, CVE-2024-35902, CVE-2024-35910, CVE-2024-35915, CVE-2024-35922, CVE-2024-35925, CVE-2024-35930, CVE-2024-35933, CVE-2024-35935, CVE-2024-35936, CVE-2024-35944, CVE-2024-35947, CVE-2024-35955, CVE-2024-35960, CVE-2024-35969, CVE-2024-35973, CVE-2024-35978, CVE-2024-35982, CVE-2024-35984, CVE-2024-35997, CVE-2024-36004, CVE-2024-36014, CVE-2024-36015, CVE-2024-36016, CVE-2024-36017, CVE-2024-36020, CVE-2024-36286, CVE-2024-36288, CVE-2024-36883, CVE-2024-36886, CVE-2024-36902, CVE-2024-36904, CVE-2024-36905, CVE-2024-36919, CVE-2024-36933, CVE-2024-36934, CVE-2024-36940, CVE-2024-36941, CVE-2024-36946, CVE-2024-36950, CVE-2024-36954, CVE-2024-36959, CVE-2024-36960, CVE-2024-36964, CVE-2024-36971, CVE-2024-37353, CVE-2024-37356, CVE-2024-38381, CVE-2024-38549, CVE-2024-38552, CVE-2024-38558, CVE-2024-38559, CVE-2024-38560, CVE-2024-38565, CVE-2024-38567, CVE-2024-38578, CVE-2024-38579, CVE-2024-38582, CVE-2024-38583, CVE-2024-38587, CVE-2024-38589, CVE-2024-38596, CVE-2024-38598, CVE-2024-38599, CVE-2024-38601, CVE-2024-38612, CVE-2024-38618, CVE-2024-38621, CVE-2024-38627, CVE-2024-38633, CVE-2024-38634, CVE-2024-38637, CVE-2024-38659, CVE-2024-38780, CVE-2024-39292) (Bug #57414)

- **linux-5.10** (CVE-2022-48655, CVE-2023-52585, CVE-2024-26900, CVE-2024-27398, CVE-2024-27399, CVE-2024-27401, CVE-2024-35848) (Bug #57434)

- **linux-latest** (CVE-2021-33630, CVE-2022-48627, CVE-2023-0386, CVE-2023-46838, CVE-2023-47233, CVE-2023-52340, CVE-2023-52429, CVE-2023-52436, CVE-2023-52439, CVE-2023-52443, CVE-2023-52444, CVE-2023-52445, CVE-2023-52449, CVE-2023-52464, CVE-2023-52469, CVE-2023-52470, CVE-2023-52486, CVE-2023-52583, CVE-2023-52587, CVE-2023-52594, CVE-2023-52599, CVE-2023-52600, CVE-2023-52601, CVE-2023-52602, CVE-2023-52603, CVE-2023-52604, CVE-2023-52609, CVE-2023-52612, CVE-2023-52615, CVE-2023-52619, CVE-2023-52620, CVE-2023-52622, CVE-2023-52623, CVE-2023-52628, CVE-2023-52644, CVE-2023-52650, CVE-2023-52670, CVE-2023-52679, CVE-2023-52683, CVE-2023-52691, CVE-2023-52693, CVE-2023-52698, CVE-2023-52699, CVE-2023-52880, CVE-2023-6040, CVE-2023-6270, CVE-2023-7042, CVE-2024-0340, CVE-2024-0607, CVE-2024-1086, CVE-2024-22099, CVE-2024-23849, CVE-2024-24857, CVE-2024-24858, CVE-2024-24861, CVE-2024-25739, CVE-2024-26597, CVE-2024-26600, CVE-2024-26602, CVE-2024-26606, CVE-2024-26615, CVE-2024-26625, CVE-2024-26633, CVE-2024-26635,

CVE-2024-26636, CVE-2024-26642, CVE-2024-26645, CVE-2024-26651, CVE-2024-26663, CVE-2024-26664, CVE-2024-26671, CVE-2024-26675, CVE-2024-26679, CVE-2024-26685, CVE-2024-26696, CVE-2024-26697, CVE-2024-26704, CVE-2024-26720, CVE-2024-26722, CVE-2024-26735, CVE-2024-26744, CVE-2024-26752, CVE-2024-26754, CVE-2024-26763, CVE-2024-26764, CVE-2024-26766, CVE-2024-26772, CVE-2024-26773, CVE-2024-26777, CVE-2024-26778, CVE-2024-26779, CVE-2024-26791, CVE-2024-26793, CVE-2024-26801, CVE-2024-26805, CVE-2024-26816, CVE-2024-26817, CVE-2024-26820, CVE-2024-26825, CVE-2024-26839, CVE-2024-26840, CVE-2024-26845, CVE-2024-26851, CVE-2024-26852, CVE-2024-26857, CVE-2024-26859, CVE-2024-26863, CVE-2024-26874, CVE-2024-26875, CVE-2024-26878, CVE-2024-26880, CVE-2024-26883, CVE-2024-26884, CVE-2024-26889, CVE-2024-26894, CVE-2024-26901, CVE-2024-26903, CVE-2024-26917, CVE-2024-26922, CVE-2024-26923, CVE-2024-26931, CVE-2024-26934, CVE-2024-26955, CVE-2024-26956, CVE-2024-26965, CVE-2024-26966, CVE-2024-26969, CVE-2024-26973, CVE-2024-26974, CVE-2024-26976, CVE-2024-26981, CVE-2024-26984, CVE-2024-26993, CVE-2024-26994, CVE-2024-26997, CVE-2024-27001, CVE-2024-27008, CVE-2024-27013, CVE-2024-27020, CVE-2024-27024, CVE-2024-27028, CVE-2024-27043, CVE-2024-27046, CVE-2024-27059, CVE-2024-27074, CVE-2024-27075, CVE-2024-27077, CVE-2024-27078, CVE-2024-27388, CVE-2024-27395, CVE-2024-27396, CVE-2024-27398, CVE-2024-27399, CVE-2024-27401, CVE-2024-27405, CVE-2024-27410, CVE-2024-27412, CVE-2024-27413, CVE-2024-27416, CVE-2024-27419, CVE-2024-27436, CVE-2024-31076, CVE-2024-33621, CVE-2024-35789, CVE-2024-35806, CVE-2024-35807, CVE-2024-35809, CVE-2024-35815, CVE-2024-35819, CVE-2024-35821, CVE-2024-35822, CVE-2024-35823, CVE-2024-35825, CVE-2024-35828, CVE-2024-35830, CVE-2024-35835, CVE-2024-35847, CVE-2024-35849, CVE-2024-35877, CVE-2024-35886, CVE-2024-35888, CVE-2024-35893, CVE-2024-35898, CVE-2024-35902, CVE-2024-35910, CVE-2024-35915, CVE-2024-35922, CVE-2024-35925, CVE-2024-35930, CVE-2024-35933, CVE-2024-35935, CVE-2024-35936, CVE-2024-35944, CVE-2024-35947, CVE-2024-35955, CVE-2024-35960, CVE-2024-35969, CVE-2024-35973, CVE-2024-35978, CVE-2024-35982, CVE-2024-35984, CVE-2024-35997, CVE-2024-36004, CVE-2024-36014, CVE-2024-36015, CVE-2024-36016, CVE-2024-36017, CVE-2024-36020, CVE-2024-36286, CVE-2024-36288, CVE-2024-36883, CVE-2024-36886, CVE-2024-36902, CVE-2024-36904, CVE-2024-36905, CVE-2024-36919, CVE-2024-36933, CVE-2024-36934, CVE-2024-36940, CVE-2024-36941, CVE-2024-36946, CVE-2024-36950, CVE-2024-36954, CVE-2024-36959, CVE-2024-36960, CVE-2024-36964, CVE-2024-36971, CVE-2024-37353, CVE-2024-37356, CVE-2024-38381, CVE-2024-38549, CVE-2024-38552, CVE-2024-38558, CVE-2024-38559, CVE-2024-38560, CVE-2024-38565, CVE-2024-38567, CVE-2024-38578, CVE-2024-38579, CVE-2024-38582, CVE-2024-38583, CVE-2024-38587, CVE-2024-38589, CVE-2024-38596, CVE-2024-38598, CVE-2024-38599, CVE-2024-38601, CVE-2024-38612, CVE-2024-38618, CVE-2024-38621, CVE-2024-38627, CVE-2024-38633, CVE-2024-38634, CVE-2024-38637, CVE-2024-38659, CVE-2024-38780, CVE-2024-39292) (Bug #57414)

- **linux-signed-5.10-amd64** (CVE-2022-48655, CVE-2023-52585, CVE-2024-26900, CVE-2024-27398, CVE-2024-27399, CVE-2024-27401, CVE-2024-35848) (Bug #57434)

- **linux-signed-amd64** (CVE-2021-33630, CVE-2022-48627, CVE-2023-0386, CVE-2023-46838, CVE-2023-47233, CVE-2023-52340, CVE-2023-52429, CVE-2023-52436, CVE-2023-52439, CVE-2023-52443, CVE-2023-52444, CVE-2023-52445, CVE-2023-52449, CVE-2023-52464, CVE-2023-52469, CVE-2023-52470, CVE-2023-52486, CVE-2023-52583, CVE-2023-52587, CVE-2023-52594, CVE-2023-52599, CVE-2023-52600, CVE-2023-52601, CVE-2023-52602, CVE-2023-52603, CVE-2023-52604, CVE-2023-52609, CVE-2023-52612, CVE-2023-52615, CVE-2023-52619, CVE-2023-52620, CVE-2023-52622, CVE-2023-52623, CVE-2023-52628, CVE-2023-52644, CVE-2023-52650, CVE-2023-52670, CVE-2023-52679, CVE-2023-52683, CVE-2023-52691, CVE-2023-52693, CVE-2023-52698, CVE-2023-52699, CVE-2023-52880, CVE-2023-6040, CVE-2023-6270, CVE-2023-7042, CVE-2024-0340, CVE-2024-0607, CVE-2024-1086, CVE-2024-22099, CVE-2024-23849, CVE-2024-24857, CVE-2024-24858, CVE-2024-24861, CVE-2024-25739, CVE-2024-26597, CVE-2024-26600, CVE-2024-26602, CVE-2024-26606, CVE-2024-26615, CVE-2024-26625, CVE-2024-26633, CVE-2024-26635, CVE-2024-26636, CVE-2024-26642, CVE-2024-26645, CVE-2024-26651, CVE-2024-26663, CVE-2024-26664, CVE-2024-26671, CVE-2024-26675, CVE-2024-26679, CVE-2024-26685, CVE-2024-26696, CVE-2024-26697, CVE-2024-26704, CVE-2024-26720,

CVE-2024-26722, CVE-2024-26735, CVE-2024-26744, CVE-2024-26752, CVE-2024-26754, CVE-2024-26763, CVE-2024-26764, CVE-2024-26766, CVE-2024-26772, CVE-2024-26773, CVE-2024-26777, CVE-2024-26778, CVE-2024-26779, CVE-2024-26791, CVE-2024-26793, CVE-2024-26801, CVE-2024-26805, CVE-2024-26816, CVE-2024-26817, CVE-2024-26820, CVE-2024-26825, CVE-2024-26839, CVE-2024-26840, CVE-2024-26845, CVE-2024-26851, CVE-2024-26852, CVE-2024-26857, CVE-2024-26859, CVE-2024-26863, CVE-2024-26874, CVE-2024-26875, CVE-2024-26878, CVE-2024-26880, CVE-2024-26883, CVE-2024-26884, CVE-2024-26889, CVE-2024-26894, CVE-2024-26901, CVE-2024-26903, CVE-2024-26917, CVE-2024-26922, CVE-2024-26923, CVE-2024-26931, CVE-2024-26934, CVE-2024-26955, CVE-2024-26956, CVE-2024-26965, CVE-2024-26966, CVE-2024-26969, CVE-2024-26973, CVE-2024-26974, CVE-2024-26976, CVE-2024-26981, CVE-2024-26984, CVE-2024-26993, CVE-2024-26994, CVE-2024-26997, CVE-2024-27001, CVE-2024-27008, CVE-2024-27013, CVE-2024-27020, CVE-2024-27024, CVE-2024-27028, CVE-2024-27043, CVE-2024-27046, CVE-2024-27059, CVE-2024-27074, CVE-2024-27075, CVE-2024-27077, CVE-2024-27078, CVE-2024-27388, CVE-2024-27395, CVE-2024-27396, CVE-2024-27398, CVE-2024-27399, CVE-2024-27401, CVE-2024-27405, CVE-2024-27410, CVE-2024-27412, CVE-2024-27413, CVE-2024-27416, CVE-2024-27419, CVE-2024-27436, CVE-2024-31076, CVE-2024-33621, CVE-2024-35789, CVE-2024-35806, CVE-2024-35807, CVE-2024-35809, CVE-2024-35815, CVE-2024-35819, CVE-2024-35821, CVE-2024-35822, CVE-2024-35823, CVE-2024-35825, CVE-2024-35828, CVE-2024-35830, CVE-2024-35835, CVE-2024-35847, CVE-2024-35849, CVE-2024-35877, CVE-2024-35886, CVE-2024-35888, CVE-2024-35893, CVE-2024-35898, CVE-2024-35902, CVE-2024-35910, CVE-2024-35915, CVE-2024-35922, CVE-2024-35925, CVE-2024-35930, CVE-2024-35933, CVE-2024-35935, CVE-2024-35936, CVE-2024-35944, CVE-2024-35947, CVE-2024-35955, CVE-2024-35960, CVE-2024-35969, CVE-2024-35973, CVE-2024-35978, CVE-2024-35982, CVE-2024-35984, CVE-2024-35997, CVE-2024-36004, CVE-2024-36014, CVE-2024-36015, CVE-2024-36016, CVE-2024-36017, CVE-2024-36020, CVE-2024-36286, CVE-2024-36288, CVE-2024-36883, CVE-2024-36886, CVE-2024-36902, CVE-2024-36904, CVE-2024-36905, CVE-2024-36919, CVE-2024-36933, CVE-2024-36934, CVE-2024-36940, CVE-2024-36941, CVE-2024-36946, CVE-2024-36950, CVE-2024-36954, CVE-2024-36959, CVE-2024-36960, CVE-2024-36964, CVE-2024-36971, CVE-2024-37353, CVE-2024-37356, CVE-2024-38381, CVE-2024-38549, CVE-2024-38552, CVE-2024-38558, CVE-2024-38559, CVE-2024-38560, CVE-2024-38565, CVE-2024-38567, CVE-2024-38578, CVE-2024-38579, CVE-2024-38582, CVE-2024-38583, CVE-2024-38587, CVE-2024-38589, CVE-2024-38596, CVE-2024-38598, CVE-2024-38599, CVE-2024-38601, CVE-2024-38612, CVE-2024-38618, CVE-2024-38621, CVE-2024-38627, CVE-2024-38633, CVE-2024-38634, CVE-2024-38637, CVE-2024-38659, CVE-2024-38780, CVE-2024-39292) (Bug #57414)

  - **nano** (CVE-2024-5742) (Bug #57399)
  - **openjdk-11** (CVE-2024-21131, CVE-2024-21138, CVE-2024-21140, CVE-2024-21144, CVE-2024-21145, CVE-2024-21147) (Bug #57511)
  - **php7.3** (CVE-2024-5458) (Bug #57400)
  - **postgresql-11** (CVE-2024-7348) (Bug #57572)
  - **pymongo** (CVE-2024-5629) (Bug #57386)
  - **python3.7** (CVE-2024-0397, CVE-2024-4032) (Bug #57477)
  - **ruby2.5** (CVE-2023-28755, CVE-2023-36617, CVE-2024-27280, CVE-2024-27281, CVE-2024-27282) (Bug #57524)
  - **systemd** (CVE-2023-50387, CVE-2023-50868, CVE-2023-7008) (Bug #57559)
  - **wpa** (CVE-2024-5290) (Bug #57519)

- UCS 5.0-9 includes the following updated packages from Debian ELTS:

  dns-root-data shim-signed atril composer dcmtk dlt-daemon dnsmasq edk2 freexian-archive-keyring frr gunicorn indent libmojolicious-perl libndp libtommath netty org-mode pdns-recursor plasma-workspace putty python-aiosmtpd python-django roundcube sendmail suricata thunderbird tryton-client tryton-server uw-imap

- The following packages have been moved to the maintained repository of UCS:

  linux-5.10 **linux-signed-5.10-amd64**

CHAPTER

TWO

DOMAIN SERVICES

- The meta-package `univention-role-server-common` now installs `linux-image-5.10-amd64` instead of `linux-image-amd64`. After the update a reboot is recommended to load the new kernel version (Bug #57427).

2.1 LDAP Directory Manager

- In case a UDM property syntax has been overridden through UCR, but the specified value doesn't correspond to any defined syntax, UDM logged a traceback. This has now been replaced by a proper log message explaining the origin of the problem (Bug #57484).
- A traceback that was thrown when running `univention-sync-memberuid` has been fixed. The script now also supports limiting operation to certain groups, or excluding certain groups (Bug #57439).
- The LDAP attribute `shadowExpire` was calculated in a way which resulted in users expiring one day later than expected in certain timezones. This has been corrected (Bug #46349).
- The UDM module `settings/directory` provides the default container setting for other UDM modules. It's now possible to extend `settings/directory` with an extended attribute to define default containers for custom UDM modules. The name of the `settings/directory` property that defines the default container for your module, can be defined by the variable `default_containers_attribute_name` in the module (Bug #57526).
- When the IP address is set when creating a new computer object, the DNS entries for this object weren't set correctly since erratum 738. The DNS entries will now be created correctly again (Bug #56313).
- When searching for objects through UDM, it was possible to create a faulty state, when an object included in the result was deleted before the operation was finished. Those deleted objects are now skipped (Bug #53333).

CHAPTER

THREE

UNIVENTION MANAGEMENT CONSOLE

3.1 Univention Portal

- All browser tabs where the user is logged into the Portal will now automatically refresh when a logout is detected. This feature is enabled by default and can be toggled with the Univention Configuration Registry Variable `portal/reload-tabs-on-logout` (Bug #57467).
- The login button in the Portal's sidebar can now be configured to perform OIDC authentication by setting the UCR variable `portal/auth-mode` to the value `oidc` (Bug #57534).
- The default for `portal/reload-tabs-on-logout` has been changed to `false` (Bug #57562).

3.2 Univention Management Console server

- Ensure that `/usr/share/univention-management-console/oidc/oidc.json` has file permission `600` (Bug #57505).
- A new endpoint has been added to the UMC, supporting the refresh of all browser tabs with the Portal open when a user logs out (Bug #57467).
- Added `oidc-id-token` hint to UMC logout to disable Keycloak's logout confirmation dialog (Bug #57475).
- Add a configurable SQL storage for UMC sessions. This now makes OIDC back-channel logout possible if the UMC is run in multiprocessing mode (Bug #57482).
- Fix a bug where it was impossible to change passwords through the UMC due to the UMC server not closing file descriptors properly (Bug #57194).
- Don't show the OpenID Connect permission consent screen when the UMC is the relying party (Bug #57506).
- Better support for Portal/UMC OIDC setup with FQDN different from internal UCS name (Bug #57483).

3.3 Univention App Center

- `univention-app configure` can now be called with `--set` being specified multiple times (Bug #57546).
- The App Center now executes the joinscript and the configure scripts during upgrade in the same order as during the initial installation (Bug #57544).

3.4 Domain join module

- A bug has been fixed that could cause the domain join to fail if the `/etc/univention/ssl` directory was too big (Bug #57421).

3.5 User management

- When a password policy is used together with the self-registration feature it was possible that invitation emails weren't sent when users are created. This was fixed by adjusting the self-service listener module filter (Bug #57226).

3.6 System diagnostic module

- The diagnostics module to check for local LDAP schema files and register them as an LDAP extension has been fixed and now actually passes the right argument to the internal function (Bug #57279).
- A diagnostic module now checks for the correct file permissions of the **`SQLite`** database of both the **`S4 Connector`** and the **`AD-Connector`** (Bug #57453).
- The package `screen` has been added to the recommendations as it's a vital part of Univention support. The package has been cut since 5.0-6 while optimizing installation size, but is now re-added. The package should be automatically installed with this update (Bug #57406).

CHAPTER

FOUR

UNIVENTION BASE LIBRARIES

- An ACL has been added that restricts access to the new UMC settings object (Bug #57482).
- A typo in evaluation of the UCR variable `backup/clean/min_backups` caused that the specified limit wasn't considered but instead the default value of `10` was applied. This has been fixed (Bug #56736).

CHAPTER

FIVE

SOFTWARE DEPLOYMENT

- The script `univention-prune-kernels` has been adjusted to the new kernel version `linux-5.10` (Bug #57427).

CHAPTER

SIX

SYSTEM SERVICES

6.1 SAML

- Prevent the creation of two mappers in the default Univention Management Console Keycloak SAML client which caused SAML logins to fail (Bug #57420).
- In `univention-keycloak`, fix the option `--no-frontchannel-logout` when dealing with OIDC Relying parties. It used to activate the front-channel logout, not deactivate it as it was supposed to do (and now does, Bug #57518).
- The `univention-keycloak` CLI was fixed, so that you can use `--set` multiple times in the `domain-config` sub command, as documented (Bug #57375).
- There was an error where a provided XML file during service provider creation overwrote the options passed on the `CLI`. This resulted in some of the migration guide example creations not working anymore (Bug #57320).
- `univention-keycloak` had to be adapted to Keycloak version 25 to correctly create the configuration for the legacy authorization (Bug #57452).

6.2 Printing services

- **`CUPS`** now uses the UCS TLS certificate instead of a self-signed certificate (Bug #52879).

CHAPTER

SEVEN

SERVICES FOR WINDOWS

7.1 Univention S4 Connector

- **SQLite** databases used by the **S4 Connector** were world readable. This has been changed (Bug #57453).
- The **S4 Connector** used to skip synchronizing a move operation, if the moved object was already present in its DN cache. This could result in the unwanted deletion of objects during a sub-tree rename (Bug #57510).

7.2 Univention Active Directory Connection

- The **AD Connector** used to skip synchronizing a move operation, if the moved object was already present in its DN cache. This could result in the unwanted deletion of objects during a sub-tree rename (Bug #57510).
- The connector can now be configured to only synchronize objects from specific sub-trees through the newly added UCR variables `connector/ad/mapping/allowsubtree/.*/ucs` and `connector/ad/mapping/allowsubtree/.*/ad`. `.*` is an arbitrary string, the value for the `ucs` variable is a sub-tree LDAP DN in the UCS directory and the value for the `ad` variable is a sub-tree LDAP DN of the AD directory. Both must include the LDAP base of the respective directory. If configured only objects from these sub-trees are synchronized, everything else is ignored (Bug #57394).
- The connector can now be configured to only synchronize objects that match a specific LDAP filter. For each object type in `user`, `group`, `container`, `ou` and `windowscomputer` the UCR variable `connector/ad/mapping/{type}/allowfilter` can be used to configure this LDAP filter (Bug #57442).
- The connector can now be configured to ignore certain objects that match a specific LDAP filter. For each object type in `user`, `group`, `container`, `ou` and `windowscomputer` the UCR variable `connector/ad/mapping/{type}/ignorefilter` can be used to configure this LDAP filter (Bug #57465).
- SQLite databases used by the AD Connector were world readable in certain cases. This has been changed (Bug #57453).
- The `dn` argument of `resync_object_from_ad.py` was set as not required (Bug #57504).

INDEX

B

C

E

P