

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 5.2-7

Release 5.2-7

22.09.2026

Die Quellen dieses Dokuments sind unter der [GNU Affero General Public License v3.0 only](#) lizenziert.

Inhaltsverzeichnis

1	Release-Highlights	3
2	Hinweise zum Update	5
2.1	Passwortauthentifizierung für deaktivierte Konten	5
2.2	Aktualisierung mehrerer UCS-Systeme	6
3	Gleichzeitiger Betrieb von UCS und Debian auf UEFI Systemen	7
4	Vorbereitung auf ein Update	9
4.1	Ausreichender Festplattenplatz	9
4.2	Nutzung der Konsole für das Update	9
4.3	Skript zur Prüfung auf bekannte Update-Probleme	9
5	Nachbereitung des Updates	11
6	Hinweise zum Einsatz einzelner Pakete	13
6.1	Erfassung von Nutzungsstatistiken	13
6.2	Empfohlene Browser für den Zugriff auf Univention Management Console	13
7	Changelog	15
8	Literaturverzeichnis	17
	Literaturverzeichnis	19
	Stichwortverzeichnis	21

Veröffentlichungsdatum von UCS 5.2-7: 2026-09-22

Release-Highlights

Univention Corporate Server 5.2-7 ist verfügbar. Es enthält Funktionsverbesserungen, Erweiterungen und Fehlerkorrekturen. Die folgende Übersicht hebt die wichtigsten Änderungen hervor:

Neues RADIUS-Authentifizierungshilfsmodul:

Die WLAN-Authentifizierung mit Benutzername und Passwort über den Nubus RADIUS-Dienst verwendet intern ein Authentifizierungshilfsmodul. Dieses Hilfsmodul hat in großen Umgebungen eine hohe CPU-Auslastung verursacht. Eine Neuimplementierung des Hilfsmoduls in Rust verringert die CPU-Auslastung und erhöht die Anzahl der Authentifizierungen, die jede UCS-Installation verarbeiten kann. Weitere Informationen finden Sie in [Bug #59042](#)¹.

Neues Guardian-Backend auf Basis von Cerbos:

Der Nubus *Autorisierungsdienst* Guardian verwendet jetzt die Open Source Lösung **Cerbos** als Backend. Es ersetzt das Open Policy Agent (OPA)-Backend. **Cerbos** enthält Funktionen, die Guardian für Autorisierungsentscheidungen benötigt. Weitere Informationen über die Autorisierungsentscheidungen werden kurz nach diesem Release im öffentlichen Univention-Blog verfügbar sein. Neben dem **Cerbos**-Backend ist der *Autorisierungsdienst* jetzt als Komponente von UCS verfügbar, die als Debian-Paket gepackt ist und einen Container enthält. Dies vereinfacht die Einrichtung und Wartung gegenüber der bisherigen Docker Compose basierten App Center App.

Verbesserte Behandlung von Passwort-Hashes und optionales Entfernen schwächerer Hashes:

Zur Vorbereitung auf die Entfernung schwächerer Passwort-Hashes enthält UCS 5.2-7 mehrere Verbesserungen. UDM bietet jetzt mehr Konfigurationsoptionen, um festzulegen, welche Hash-Algorithmen beim Speichern von Passwörtern verwendet werden. Mit diesen Optionen können Sie schwächere Hashes entfernen, die aus Kompatibilitätsgründen weiterhin gespeichert werden. Die Active Directory Verbindung unterstützt jetzt mehr Konfigurationen, bei denen Active Directory mit reduzierten Verschlüsselungstypen konfiguriert ist.

Keycloak-Metriken:

Die Keycloak App ermöglicht jetzt die Aktivierung des integrierten „Metrics Endpoint“ in Keycloak. Administratoren erhalten detaillierte Informationen über die Nutzung von Keycloak und Ereignisse in ihren Prometheus- und Grafana-Dashboards. Weitere Informationen finden Sie in [Monitoring Keycloak with metrics](#)² in *Univention Keycloak app documentation* [1].

Unterstützung für Bildungsklassen im Microsoft 365 Connector:

Der *Microsoft 365 Connector* ermöglicht jetzt die Aktivierung von „Bildungsklassen“ in Microsoft 365. Administratoren von Nubus oder UCS@school können festlegen, welche Gruppen automatisch aktiviert werden,

¹ https://forge.univention.org/bugzilla/show_bug.cgi?id=59042

² <https://docs.software-univention.de/keycloak-app/latest/use-cases.html#use-case-metrics-monitoring>

sodass sie die Funktion nicht manuell in Microsoft 365 verwalten müssen. Weitere Informationen finden Sie in [Bildungsklassen](#)³ im *UCS Handbuch* [2].

³ <https://docs.software-univention.de/manual/5.2/de/idm-cloud/office-365.html#idmcloud-o365-education-classes>

Hinweise zum Update

Bevor Sie aktualisieren, testen Sie das Update in einer separaten Testumgebung, die mit Ihrer Produktionsumgebung identisch ist. Führen Sie das Update in einem Wartungsfenster durch, da einige Dienste in der Domäne vorübergehend nicht verfügbar sein können.

Je nach Systemleistung, Netzwerkverbindung und installierter Software kann die Aktualisierung zwischen 30 Minuten und mehreren Stunden dauern. Für große Umgebungen konsultieren Sie bitte den *UCS performance guide* [3].

2.1 Passwortauthentifizierung für deaktivierte Konten

Seit UCS 5.2-7 macht das Deaktivieren eines Benutzerkontos dessen Passwort-Hash nicht mehr ungültig. UCS setzt die Kontodeaktivierung während eines LDAP-Binds durch. Eine serverseitige Prüfung weist deaktivierte Konten zurück.

Warnung

Dienste, die den Passwortabrufmodus verwenden, können deaktivierte Konten weiterhin authentifizieren. Aktualisieren Sie ihre Authentifizierungskonfiguration, um den Zugriff zu verhindern.

Die folgenden von UCS unterstützten Dienste und Apps sind nicht betroffen und erfordern keine Änderungen durch den Betreiber:

- Dienste, die sich über einen LDAP-Bind authentifizieren.
- Dienste, die token- oder OIDC-basierte Authentifizierung verwenden.
- OX App Suite auf UCS.
- Standard UCS-Maildienste.

Dienste im Passwortabrufmodus lesen den `userPassword`-Hash und prüfen ihn lokal, anstatt einen Benutzer-Bind durchzuführen. Beispielsweise verwendet Dovecot den Passwortabrufmodus ohne `auth_bind = yes`.

Wenn Sie einen Dienst betreiben, der den Passwortabrufmodus verwendet, führen Sie einen der folgenden Schritte durch:

1. Wechseln Sie zur LDAP-Bind-Authentifizierung. Zum Beispiel für Dovecot, setzen Sie `auth_bind = yes`.
2. Aktualisieren Sie den LDAP-Suchfilter, um deaktivierte Konten auszuschließen, beispielsweise mit `(!(krb5KDCFlags:1.2.840.113556.1.4.803:=128))`.

2.2 Aktualisierung mehrerer UCS-Systeme

In Umgebungen mit mehreren UCS-Systemen muss der Primary Directory Node bei einem Release-Update immer das erste System in der Aktualisierungsreihenfolge sein.

Weitere Informationen zur Planung von Updates in Multiserver Umgebungen finden Sie unter [Planning updates in multiserver environments](#)⁴ im *Nubus für UCS 5.2 - Betriebshandbuch* [4].

⁴ <https://docs.software-univention.de/ucs-operation/5.2/en/lifecycle/update-strategies.html#lifecycle-update-strategies-multiple-systems-environments>

Gleichzeitiger Betrieb von UCS und Debian auf UEFI Systemen

Der gleichzeitige Betrieb von UCS und Debian GNU/Linux auf UEFI-Systemen wird seit UCS 5.0 nicht mehr unterstützt.

Der GRUB-Bootloader von Univention Corporate Server verwendet dieselben Konfigurationsdateien wie Debian. Wenn Debian bereits installiert ist, kann UCS nach der Installation oder dem Update auf UCS 5.0 nicht starten. Umgekehrt verhindert die Installation von Debian nach der Installation von UCS 5.0, dass UCS startet.

Weitere Informationen finden Sie in [KB 17768](https://help.univention.com/t/17768)⁵.

⁵ <https://help.univention.com/t/17768>

Vorbereitung auf ein Update

In diesem Abschnitt finden Sie wichtige Überlegungen vor dem Update.

4.1 Ausreichender Festplattenplatz

Stellen Sie sicher, dass Sie ausreichend Festplattenplatz für das Update haben. Eine Standardinstallation benötigt 6 bis 10 GB. Der Update-Prozess benötigt zusätzlich 1 bis 2 GB, um Pakete herunterzuladen und zu installieren, abhängig von der Größe Ihrer vorhandenen Installation.

4.2 Nutzung der Konsole für das Update

Melden Sie sich für das Update auf der lokalen Konsole des Systems mit dem Benutzer `root` an und starten Sie das Update dort. Alternativ können Sie das Update über Univention Management Console durchführen.

Wenn Sie das Update über eine Netzwerkverbindung durchführen, ergreifen Sie Maßnahmen, um sicherzustellen, dass es bei einer Unterbrechung der Verbindung weiterläuft. Netzwerkunterbrechungen können das Update abbrechen, was das System erheblich beeinträchtigt.

Verwenden Sie Tools wie `tmux`, `screen` oder `at`, damit das Update auch bei Netzwerkunterbrechungen weiterläuft. Alle UCS-Systemrollen haben diese Tools standardmäßig installiert.

4.3 Skript zur Prüfung auf bekannte Update-Probleme

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

```
# download
$ curl -Oof https://updates.software-univention.de/download/univention-update-
↪checks/pre-update-checks-5.2-7{.gpg,}

# verify and run script
$ apt-key verify pre-update-checks-5.2-7{.gpg,} && bash pre-update-checks-5.2-7
...

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
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  
...
```

Nachbereitung des Updates

Führen Sie nach dem Update neue oder aktualisierte Join-Skripte aus. Verwenden Sie dazu entweder das Verwaltungsmodul *Domain join* in der *Management UI* oder führen Sie **univention-run-join-scripts** als `root` aus.

Prüfen Sie, ob die Join-Skripte erfolgreich abgeschlossen wurden. Starten Sie dann das UCS-System neu.

Hinweise zum Einsatz einzelner Pakete

Die folgenden Abschnitte informieren über ausgewählte Pakete dieses Updates.

6.1 Erfassung von Nutzungsstatistiken

Wenn Sie UCS Core Edition verwenden, erfasst UCS anonyme Nutzungsstatistiken für Univention Management Console. Das System protokolliert die Module, die Sie öffnen, in einer *Matomo*-Instanz. Diese Statistiken helfen Univention, die Entwicklung von Univention Management Console anhand der Kundenanforderungen zu verbessern.

Sie können den Lizenzstatus über den Menüeintrag *Lizenz* ▶ *Lizenzinformationen* im Benutzermenü von Univention Management Console überprüfen. Wenn die *Lizenzinformationen* unter *Lizenztyp* UCS Core Edition auführen, verwendet Ihr UCS-System die UCS Core Edition.

UCS sammelt keine Nutzungsstatistiken, wenn Sie eine *Enterprise Subscription*⁶-Lizenz wie *UCS Base Subscription* oder *UCS Standard Subscription* nutzen.

Unabhängig von Ihrer Lizenz können Sie die Erfassung von Nutzungsstatistiken deaktivieren, indem Sie die Univention Configuration Registry Variable `umc/web/piwik` auf `false` setzen.

6.2 Empfohlene Browser für den Zugriff auf Univention Management Console

Univention Management Console verwendet JavaScript- und CSS-Funktionen, um die Web-Oberfläche darzustellen. Ihr Webbrowser muss Cookies unterstützen. Univention Management Console benötigt einen der folgenden Browser:

- Chrome Version 131 und höher
- Firefox Version 128 und höher
- Safari und Safari Mobile Version 18 und höher
- Microsoft Edge Version 128 und höher

Ältere Browser können die Web-Oberfläche fehlerhaft darstellen oder Funktionsstörungen verursachen.

⁶ <https://www.univention.com/products/prices-and-subscriptions/>

KAPITEL 7

Changelog

Die Änderungen seit UCS 5.2-6 finden Sie in [Changelog for Univention Corporate Server \(UCS\) 5.2-7](https://docs.software-univention.de/changelog/5.2-7/en/index.html)⁷.

⁷ <https://docs.software-univention.de/changelog/5.2-7/en/index.html>

KAPITEL 8

Literaturverzeichnis

Literaturverzeichnis

- [1] *Univention Keycloak app documentation*. Univention GmbH, 2023. URL: <https://docs.software-univention.de/keycloak-app/latest/>.
- [2] *UCS Handbuch*. Univention GmbH, 2021. URL: <https://docs.software-univention.de/manual/5.2/de/>.
- [3] *UCS performance guide*. Univention GmbH, 2021. URL: <https://docs.software-univention.de/ext-performance/5.2/en/index.html>.
- [4] *Nubus für UCS 5.2 - Betriebshandbuch*. Univention GmbH, 2025-2026. URL: <https://docs.software-univention.de/ucs-operation/5.2/de/>.

B

Bugzilla
Bug #59042, [3](#)

K

Knowledge Base
KB 17768, [7](#)

U

umc/web/piwik, [13](#)
Umgebungsvariable
umc/web/piwik, [13](#)