

Release Notes

Software Version: V3R0.95.0, 2025-05-04

Unify Phone

Current release status can be verified via the Software Supply Server (SWS)

© Copyright, Unify Software and Solution GmbH & Co. KG All rights reserved.

This document provides general information about the release, generics, and other relevant notes for the corresponding product and its correction versions.

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Table of Contents

1	HISTORY OF CHANGE	2
1.1	RELEASE NOTES CONTENT.....	2
1.2	PRODUCT VERSIONS HISTORY	3
2	CHANGES	3
2.1	IMPLEMENTED CHANGE REQUESTS / NEW FEATURES.....	3
2.2	RESOLVED REPORTED PROBLEMS / SYMPTOMS	3
2.3	RESOLVED VULNERABILITIES	3
3	IMPORTANT ISSUES, WORKAROUNDS, HINTS AND RESTRICTIONS TO A SPECIFIC RELEASE ..	4
3.1	IMPORTANT ISSUES	4
3.2	WORKAROUNDS, HINTS	4
3.2.1	<i>Troubleshooting issues</i>	<i>4</i>
3.2.2	<i>Xiaomi Devices - Granting additional app permissions</i>	<i>4</i>
3.3	RESTRICTIONS.....	5
4	HARDWARE AND SOFTWARE COMPATIBILITY	5
4.1	HARDWARE.....	5
4.2	FIRMWARE.....	5
4.3	LOADWARE.....	5
4.4	SOFTWARE / APPLICATIONS	5
4.4.1	<i>Software components included in this release</i>	<i>5</i>
4.5	OPERATING SYSTEMS	5
4.6	COMPLIANT PRODUCTS	5
4.6.1	<i>Communication platforms</i>	<i>5</i>
4.6.2	<i>Other products</i>	<i>6</i>
4.6.3	<i>Third-Party products</i>	<i>6</i>
5	ADDITIONAL INFORMATION	6

1 History of Change

1.1 Release notes content

Version	Date	Description of changes
1.0	2025-04-28	Initial version for V3R0.95.0

1.2 Product versions history

Software Version	Production Version	Date	Remarks
V3R0.86.0		2024-12-15	
V3R0.87.0		2025-01-12	
V3R0.88.0		2025-01-26	
V3R0.89.0		2025-02-09	
V3R0.90.0		2025-02-23	
V3R0.91.0		2025-03-09	
V3R0.92.0		2025-03-23	
V3R0.93.0		2025-04-06	
V3R0.94.0		2025-04-27	
V3R0.95.0		2025-05-04	

2 Changes

2.1 Implemented Change Requests / New features

Not applicable for this release.

2.2 Resolved Reported Problems / Symptoms

Not applicable for this release.

2.3 Resolved Vulnerabilities

Tracking Reference	Summary	Released in Version
CVE-2025-2559	A flaw was found in Keycloak. When the configuration uses JWT tokens for authentication, the tokens are cached until expiration. If a client uses JWT tokens with an excessively long expiration time, for example, 24 or 48 hours, the cache can grow indefinitely, leading to an OutOfMemoryError. This issue could result in a denial of service condition, preventing legitimate users from accessing the system.	V3R0.95.0
CVE-2025-1391	A flaw was found in the Keycloak organization feature, which allows the incorrect assignment of an organization to a user if their username or email matches the organization's domain pattern. This issue occurs at the mapper level, leading to misrepresentation in tokens. If an application relies on these claims for authorization, it may incorrectly assume a user belongs to an organization they are not a member of, potentially granting unauthorized access or privileges	V3R0.95.0

CVE-2025-11734	A denial of service vulnerability was found in Keycloak that could allow an administrative user with the right to change realm settings to disrupt the service. This action is done by modifying any of the security headers and inserting newlines, which causes the Keycloak server to write to a request that has already been terminated, leading to the failure of said request.	V3R0.95.0
CVE-2025-11736	A vulnerability was found in Keycloak. Admin users may have to access sensitive server environment variables and system properties through user-configurable URLs. When configuring backchannel logout URLs or admin URLs, admin users can include placeholders like \${env.VARNAME} or \${PROPNAME}. The server replaces these placeholders with the actual values of environment variables or system properties during URL processing.	V3R0.95.0
CVE-2025-24970	Netty, an asynchronous, event-driven network application framework, has a vulnerability, when a special crafted packet is received via SslHandler, it doesn't correctly handle validation of such a packet in all cases which can lead to a native crash.	V3R0.95.0

3 Important Issues, Workarounds, Hints and Restrictions to a specific release

This section provides the latest information at time of software release and is only pertaining to the time of release notes generation.

3.1 Important Issues

Not applicable for this release.

3.2 Workarounds, Hints

3.2.1 Troubleshooting issues

In the link below you may find the Troubleshooting Guide for Unify Phone
<https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/59a4c308-57f9-46a6-b4c0-d05a44d99711>

3.2.2 Xiaomi Devices - Granting additional app permissions

For Unify Phone to work properly on a Xiaomi device, you need to manually grant the app with a set of UI permissions.

- 1) To allow Unify Phone to use the background autostart service:
 - a) On your device **Settings**, navigate to **Apps > Permissions > Autostart**.
 - b) Switch the slider next to Unify Phone to **ON**.
- 2) To allow Unify Phone to show notifications on phone's lock screen:
 - a) On your device **Settings**, navigate to **Apps > Permissions > Other permissions**.
 - b) Tap **Permissions > Show** on Lock screen.
 - c) Enable the checkbox next to Unify Phone.

These steps may vary depending on the MIUI version.

3.3 Restrictions

Not applicable for this release.

4 Hardware and Software Compatibility

4.1 Hardware

Not applicable for this release.

4.2 Firmware

Not applicable for this release.

4.3 Loadware

Not applicable for this release.

4.4 Software / Applications

4.4.1 Software components included in this release

Released with	Component	Version
V3R0.95.0	Web Client	4.2.201
V3R0.95.0	Android Client	3.0.95.1
V3R0.95.0	iOS Client	3.0.95

Mobile app availability is subject to Apple's and Google's release process for the respective app stores.

4.5 Operating systems

Below are the Operating System versions supported by Unify Phone mobile clients.

Component	Minimum Supported Version	Latest Supported Version
Android Client	Android 10	Android 14
iOS Client	iOS 16	iOS 18

4.6 Compliant products

This section lists the versions associated with the communication platforms, other products and third-party products that have been tested for use with this version of the product and are known to work.

4.6.1 Communication platforms

Product Family	Product	Verified Software Versions		
		Version	Status	NUXEO Note
OpenScape Voice	OpenScape Voice	V10R3.33.3	GA	Check SWS
OpenScape 4000	OpenScape 4000	V11R0.22 CSTA HF3 RMX HF10	GA	Check SWS

Product Family	Product	Verified Software Versions		
		Version	Status	NUXEO Note
		LW HF7		
SBC	SBC	V11 R2.01.01	GA	Check SWS
OpenScape Business	OSBiz X OSBiz S	V3 R4.0.1.006 V3 R4.0.1.006	HF	Check SWS
MiVoice	MiV5000	A5000 R8.2 SP3 /B400	GA	
OpenScape Common Management Platform	OpenScape Common Management Platform	V10R5 FR15	GA	Check SWS

The current Common Compatibility Matrix can be found on the Mitel Unify Partner Portal

<https://www.mitel.com/login/unify-login>.

Note: Use the "Search" option and Search Documents for "Common Compatibility Matrix" (select "Search on title only").

4.6.2 Other products

Not applicable for this release.

4.6.3 Third-Party products

Not applicable for this release.

5 Additional Information

Unify Phone Connector status and potential alerts can be found under:

<https://status.mitel.io/>