



Product Support Notice

© 2023 Avaya LLC. All Rights Reserved.

PSN# PSN006220u

Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: October 23, 2023. This is Issue #01, publication date: October 23, 2023

Severity/risk level

High

Urgency

When convenient

Name of problem

Upcoming Release of Avaya Workplace 3.35

Products affected

- Avaya Workplace for Windows
- Avaya Workplace for iOS
- Avaya Workplace for Android
- Avaya Workplace for macOS

Problem description

This PSN advises customers and partners of the upcoming release of Avaya’s Workplace software clients. This release is expected to be available on 24th October for **Windows and Android** platforms.

For iOS, it is targeted to be released in second week of November between 7th and 10th, 2023, on app store.

The iOS updates will be available from the mobile app stores, subject to app-store approval timelines.

Avaya Workplace for MacOS will be released on 31st October.

In addition to bug fixes and other enhancements, the following new features are provided with 3.35:

Feature	Platform(s)
VDI Paired Sign-on session Quick Change when moving between thin clients	Windows
Enhancement to increase the Workplace font size	Windows
Send-NN feature button	Windows, Android, iOS
Display conversation messages separately, do not merge them in a single message	Windows, Android, iOS
Support TLS 1.3	MacOS, iOS
Presence Access Control (ACL) to be supported on Workplace Mobile clients	Android, iOS
Enhancement SIP shared control: Service observe	Windows
Support different Matching Criteria for Greetings including UI	Windows

Resolution

Avaya has aimed to make Avaya Workplace highly backwards compatible with existing deployments and settings configurations. If you do not wish for mobile clients to update to a new version when published to the mobile app stores, ensure that auto-update is disabled for all devices in use. Android supports the ability to disable auto-updates on a per-app basis, and iOS requires auto-updates to be managed at the device level.

Workaround or alternative remediation

Remarks

n/a

Patch Notes

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

n/a

Service-interrupting?

n/a

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

n/a

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support [Terms of Use](#).

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA LLC, ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya LLC.

All other trademarks are the property of their respective owners.