Omnissa Workspace ONE UEM Release Notes

Version: 2509 | Last Updated Feb 3, 2026 | 11 minute read | Summarize |

Omnissa Workspace ONE UEM | Release Notes | 2509

We're excited to share the new release of Workspace ONE UEM version 2509! Read on to learn about the new features and improvements in this release.

: **Urgent Notification regarding legacy Domain End of Service**
As part of the migration from legacy VMware-owned domains to Omnissa-owned domains, customer networkand security teams must make firewall changes to allow access to the new Omnissa-owned domains byJune 15th, 2025,to prepare and not block the new Omnissa domain network requests in upcoming product and service updates. This also impacts any API driven tasks or automation tasks created. Please see KB6000840 for more information.

What's New in this Release

Admin Experience

Read-Only Access Control for Settings

You can now create custom administrator roles with read-only permissions for all **Settings** in Workspace ONE UEM. This feature enables users to view every settings page without modifying or interacting with configurations. It improves visibility and audit capabilities while maintaining configuration integrity.

Android Management

Set WiFi roaming behavior (Custom DPC) on your devices

You can now configure device roaming between access points while connected to WiFi networks. For a specific network, you can enable more aggressive roaming to prioritize signal strength over battery consumption. This feature is supported on Work-Managed and Corporate Owned Personally Enabled (COPE) devices running Android 15 and higher.

Certificate Management

Customizable SID mapping in OID/SAN certificate attributes

Omnissa has enhanced the configuration capabilities for SID mappings within the OID/SAN certificate template attributes. The latest implementation introduces support for overriding the default user-based SID configuration, allowing administrators to define a fixed SID or substitute it with a custom variable, such as the newly introduced `ComputerSID`. This enhanced configurability enables organizations to meet additional advanced mapping requirements by offering greater flexibility in SID assignment.

Console Settings

Bring Your Own Key (BYOK): Take control of your data security

Workspace ONE UEM Preferred SaaS now supports Bring Your Own Key (BYOK), allowing organizations to manage their own RSA-4096 wrapped Key Encryption Keys (KEKs) for data-at-rest encryption. BYOK not only provides encryption but also empowers organizations to define their own security rules and maintain control over their keys. The key capabilities include:

- **Customer-Controlled KEK**: Organizations using Customer-controlled KEK can manage their own Key Encryption Keys (KEK), set renewal schedules, and control encryption lifecycle operations.
- **Secure Storage**: Omnissa securely stores the KEK in a Hardware Security Module (HSM), ensuring limited system access to the root of trust.

ON THIS TOPIC

- **Auditability**: All key access and encryption operations are fully auditable, supporting governance and compliance requirements.
- **Zero Trust Alignment**: The BYOK lays the foundation for Zero Trust architecture, enabling agile adaptation to evolving security models and technologies.

For more information, see Bring Your Own Key (BYOK) Support for Workspace ONE UEM Preferred SaaS.

Improved Device and Console log collections

Workspace ONE UEM brings you an upgrade with enhanced log collection. It now supports one-click-log-collection, gathering all logs, including server and device application logs (Hub, Boxer, Tunnel, etc.). You can target Console or Services logs or start at the Device context. This process enhances the support experience and simplifies troubleshooting by ensuring log captures include all necessary information on the first attempt, preventing the need for multiple log-gathering requests. Logs collected are now accessible to Omnissa Support teams through internal tools.

Freestyle Orchestrator

Quick and easy app and profile removal for Freestyle Orchestrator Mobile

You can now create a workflow that includes a step to remove an application and/or profile from iOS and Android devices. When the workflow is deployed, the specified app or profile will be removed from the device. For more information, see Remove Applications and Profiles from Mobile Devices using Workflows.

Streamline onboarding entitlements in workflows for macOS

Onboarding entitlements within workflows are now supported on macOS with **Limited Availability**. This feature allows administrators to prioritize resources essential for onboarding, which take precedence over other resource assignments. To have this feature enabled for your environment, contact your account team.

ARM64 support for macOS

The workflow engine is now fully ARM64 compatible, eliminating the need for Rosetta translation on Apple Silicon devices.

macOS Management

Faster FileVault recovery key escrow for macOS enrollment

The time required for a macOS device to escrow the FileVault recovery key into Workspace ONE UEM during enrollment has been reduced. This change allows for quicker access to the key, facilitating immediate viewing following enrollment. Previously, if a user forgot their password after setup, the device would lock and the recovery key would not yet be available in the console. Now, a quick escrow process ensures the FileVault recovery key is escrowed right after you activate it at the Setup Assistant. This improves the user experience.

Resource Management

Real-time app assignment status in Device Details

You can now view app assignment status in real-time within the **Apps** tab of a **Device Details** view. This enhancement provides immediate visibility into app assignment status, reducing troubleshooting delays and helping you act faster. This capability is currently in **Limited Availability**. To have it enabled for your environment, contact your account team.

Installation metrics now retained upon Resource and Smart group updates

When assignment or payload updates are made to apps and profiles, or when their assigned Smart groups are modified and republished, installation metrics achieved so far will now be retained and remain visible on the Deployment Tracking page as **Currently assigned**. It denotes all devices having a confirmed assignment to an app or profile at any given time. This enhancement is currently being rolled out on a Limited Availability basis starting with Patch 1. If you are interested in an early access, get in touch with your account team.

Faster resource delivery for larger device populations

Faster resource delivery is now supported for a larger device population when apps and profiles are published. This type of delivery is initiated whenever new apps or profiles are published, assignments for

existing ones are updated, profile payloads are modified, or Smart Group rules change if the number of devices impacted by such updates is below a defined threshold. Devices impacted by these updates will check in immediately and install or remove the necessary resources instead of waiting for the standard check-in cycle. This enhancement is being rolled out on **Limited Availability** starting **2509 Patch 3**. Contact your Account Team if you would like to participate in the Limited Rollout or have any questions regarding this enhancement.

Windows Management

Enhanced version management for Hub and improved ARM integration within Workspace ONE UEM
You can now choose the Intelligent Hub version directly from the Workspace ONE UEM Console, eliminating the need to repackage and deploy the installer for each new release.

Key features include:

- **Flexible version management**: Select the Intelligent Hub version for deployment, including:
  - GA version (General Availability)
  - Beta version (for testing and validation in specific Organizational Groups)
- **Win32 and ARM support**: Full support for Win32 and ARM-based devices is available in all deployment scenarios.

For more information, see Intelligent Hub Application Version Control and Intelligent Hub Application topics.

Streamline application management with Enterprise Application Repository v2 (EARv2)
This **Limited Availability** feature simplifies how administrators discover, configure, and deploy over 8000 enterprise applications for Windows devices in Workspace ONE UEM. The new Enterprise Application Repository (EAR) provides a centralized, secure source of pre-vetted applications that can be managed directly from the UEM Console, minimizing manual packaging and configuration.

- **Centralized Application Catalog**: Easily navigate, search, and add trusted applications from the Enterprise Application Repository directly from the UEM Console.
- **Automated Configuration**: The repository automatically generates commands to install, uninstall, and detect, reducing manual setup and improving consistency.
- **Brownfield App Linking**: Existing (manually uploaded) applications can now be linked to the repository for automatic version tracking and update visibility.
- **Seamless Updates**: Initiate updates directly from the console, facilitating continuous application maintenance with minimal effort.

For more information, see Add Windows applications from the Enterprise Application Repository.

Resolved Issues

Admin Experience

- FCA-210682: Custom message templates in deprecated languages cannot be edited.
- FCA-210742: Errors while navigating to different pages in the UEM console.
- FCA-210698: Incorrect Exception seen when API returns a 400 Bad Request for some scenarios.
- FCA-210746: License count not properly reflecting in the UEM Admin Panel.
- FCA-207442: Problem arises from the JavaScript implementation where the ‘testCookie’ is set without explicitly defining the attributes.

Android Management

- AGGL-18872: DB script does not handle nvarchar to datetime conversion properly for all date formats.

Common Services

- CMSVC-20517: Error occurs while creating OAuth token in Partner OG.

Content Infrastructure

- CMCM-191349: Facing issues while accessing “Content Dashboard” with “Content Management” Admin role.

Core Platform

- CRSVC-63683: Unable to filter console logs by searching the Account name.
- CRSVC-64367: Resource delivery is not unblocked when a device becomes Compliant for a policy with Block/Remove resource actions.
- CRSVC-66909: API call counter was not reporting usage as expected.

Enrollment and Service Integrations

- ESI-563: Devices are not being assigned the correct Ownership Type.
- ESI-603: Deleting a device on Self Service portal shows error message.
- ESI-615: Unable to add Custom User groups for enrollment restrictions.
- ESI-710: Unable to bulk remove device registration tokens.
- ESI-711: “Registration” page title changes to “Enrollment Status” after performing action.
- ESI-775: Staging user enrolment failing for multiple platforms.

Freestyle Orchestrator

- FS-7946: UEM update trigger in-scope workflow/script for macOS unexpectedly.
- FS-8071: Fix error while consuming feedback for workflow step keeping workflow stuck in progress.

iOS Management

- AAPP-19306: Cannot edit a profile with exchange ActiveSync/Subscribed Calendar iOS payload.
- AAPP-19829: Shared iPads for Business experience delays in resource delivery when switching users.
- AAPP-20057: Device enrollment failures for iOS 18.6.2 when OS restriction policy is enforced.

Resource Management

- ARES-31936: Profile does not get installed on devices with ‘Auto’ direct assignment unless the On-demand workflow is manually triggered.
- ARES-33173: Spaceman error is displayed when clicking ‘View’ on the Profile List.
- ARES-33301: App scheduled for future deployment installs immediately.
- ARES-33361: Device Details view displays incorrect profile summary counts.
- ARES-33426: Deleted and deactivated profiles visible on Device Profiles list.
- ARES-33466: Existing assignments displayed as ‘Added’ in assignment preview while republishing Web Link.
- ARES-33477: A few profiles unintentionally installed on Smart Groups if it were previously assigned to it through a now-deleted Workflow.
- ARES-33610: Assignment and installation data misreported for devices assigned to Internal app versions with exclusions.
- ARES-34443: Admin occasionally unable to save assignments for Android Internal Apps.
- ARES-34450: Installation Status Last Scan on Device App list sometimes displays future time.

- ARES-34502: Received ‘Something unexpected happened’ error while exporting App log from UEM Console.
- ARES-34536: Trusted Credentials setting under Wifi payload cannot be saved in DDUI Profiles.
- ARES-34857: ‘Failed to save profile’ error may occur when publishing a profile whose payload has not been updated.

User Management

- UM-10250: User Groups List View does not load results beyond selected page size.
- UM-10252: Clear and Save is failing for both ‘Service Provider (AirWatch) Certificate’ and ‘Identity Provider Certificate’.

Windows Management

- AMST-44769: Windows Autopilot enrollment stuck at OOBE “Setting up Work or School” screen after patch 24 upgrade.
- AMST-44385: App removal failing instantly for a Windows internal application.
- AMST-45025: Device reassignment is failing intermittently for with a specific set of users.

Patch Resolved Issues

Patch 1

- FS-8831: Enhanced error handling for socket exceptions to prevent silent failures during script execution.
- FS-8564: Scripts unable to execute due to an unexpected reboot causing a corrupted DB on macOS devices.
- FCA-211680: Add link to collect logs in the user details dropdown.
- ATL-27185: Seed Machost v2509.4802 to 2509 patch 1.
- ATL-27071: Seed Workspace ONE Intelligent Hub v25.06.5 for Windows to UEM 2509.
- ARES-35268: Apps delivered through Product Provisioning removed from devices when they lose assignment.
- ARES-34933: “An error has occurred” sometimes appears while performing actions related to apps and profiles.
- AGGL-19412: Outdated settings shown when viewing ChromeOS Credentials profiles.
- AAPP-20600: Device Updates page failing to load new versions (iOS/macOS).
- AAPP-20593: Fix SKU mapping for Device Attestation and Release Device from ABM.
- AAPP-20016: Apple TV - VPP License is not revoked after removing app from Device Details page.

Patch 2

- MACOS-6589: New versions of native Mac app uploads improperly handling rebranded (com.ws1) Bundle ID.
- FS-8580: Workflow fails on macOS 26 RC 1 devices due to step timeout persisting after completion.
- ESI-825: MTD Activation through Smart Groups fail when deployed from Partner tenant.
- CRSVC-70627: Tunnel App showing Access Denied until reinstalled.

- CMCM-191640: Admin repo empty after clicking on 'sign-in' in Content app.
- ATL-27265: Seed - Machost 2509.4939 to Workspace ONE UEM 2509.
- ARES-35269: Error occurs intermittently while viewing Profile List View.
- AGGL-19570: Per-app VPN settings not working when VPN profile includes additional payloads.
- AGGL-19522: After running the seed script, the API level for Android 16 is displayed as null.
- AAPP-20322: iOS Device Updates details page update-status grid filters are not functioning as expected.
- AAPP-20207: VPP application versions are not updating in the Console when the country code is non-English.
- AAPP-19914: Workspace ONE UEM Console inherit setting blocked for Apple -> SCEP.
- RUGG-13731: Repeated product delivery and device reboots when Reboot Manifest is used with other actions.

Patch 3

- RUGG-13764: Device level update status for Custom Update is not syncing after update is marked completed.
- LUEM-963: Software Update Profile for Linux devices.
- FCA-211628: 'Logging Server Failure' notification preferences are not seen in Account Settings.
- FCA-211339: Update mdm/device/search v2 API to add field for reporting physical memory with the memory unit.
- ESI-834: Azure AD token not revoked when device is unenrolled or wiped.
- ESI-644: Android devices enroll without a registration record.
- CRSVC-71133: Resolved scenario where profiles using SCEP certificates may not install correctly for newly enrolled macOS devices.
- CRSVC-70627: Tunnel app showing Access Denied on rapid check-in/checkout of shared Android device.
- CRSVC-70337: Improved logic for device command queue stored procedure related to application removal protection.
- CRSVC-55456: Resolved inconsistency between the Certificate list API and UI.
- CMCM-191535: Unable to access network shares on Content app post UEM upgrade to 24.10.
- ATL-27303: Seeding macOS Hub 25.11 to UEM 25.09 patch 3.
- ATL-27297: Seed Workspace ONE Intelligent Hub v25.06.6 for Windows to 2509.
- ARES-34394: Incorrect admin reported for some device troubleshooting log events.
- AMST-45190: Handle Device Reassignment failures with internal server error.
- AAPP-20421: 500 Error on Purchased App API Endpoint (/mam/apps/purchased/search).
- AAPP-20216: Editing iOS VPN profile requires selecting duplicate DTR fields.

- AAPP-19962: VPP V2 - Unenrollment of the primary device of a Shared User Based License is not working as expected.

Patch 4

- FS-8392: Kafka exploratory work with FIPS.
- ATL-27493: Seed - Machost to canonical release PR2509-3.
- ATL-27460: Seed Workspace ONE Intelligent Hub verson 25.06.7 for Windows to 2509.
- ARES-36022: Save Failed error received when trying to publish an app assignment with the App Config included.
- ARES-35570: Google pPayload Declarative profile fails to save.
- ARES-34664: 'Installed Date' column is blank in Profile Details by Device report.
- ARES-34608: View counts on App list do not match with Deployment Tracking after updating assignments.
- AMST-45464: Main - DropshipProvisioning- Backport Dropship items.
- AMST-45408: Windows Device Reassignment is failing with HybridAD setup.
- AMST-44772: Higher level OG assigned domain join configuration not found at lower OG.
- AAPP-20636: Add timeouts and additional diagnostics for APNS processing.
- AAPP-20276: Support for new Web Content Filter keys introduced in Apple OS 26.
- AAPP-20190: Incorrect calculation of allocated and redeemed VPP counts resulting in a negative unallocated count.

Patch 5

- PPAT-20873: Tunnel DTR access issue.
- CRSVC-68243: Certificate Profile option in Certificate Template does not retain setting after it is saved and reopened.
- ARES-36022: Save Failed error when trying to publish an app assignment with the App Config included.
- ARES-34664: 'Installed Date' column is blank in Profile Details by Device report.

Patch 6

- SINST-176707: Corrected a condition in which the updated ACC Installation Directory was not honored.
- LUEM-1060: Intel WF that installs profiles on devices does not work.
- ESI-892: Possible gaps in Enrollment Status writes to DST.
- CRSVC-71542: Compliance actions are not reverted after concurrency exception.
- CRSVC-70502: Fix read readiness flag caching and no tenant enablements.

Known Issues

FS Mobile: Outdated Assignment Status on Legacy Screens

Some legacy screens may not accurately show the status of app/profile assignments when resources are removed through a mobile workflow. For example, the legacy App Catalog and Intelligence dashboards prior to ETLv2 may display outdated assignment information.

Workaround

Upgrade to use the latest modstack-compatible features, such as the Hub Services App Catalog and ETLv2 as it becomes available, to ensure assignment statuses are displayed correctly.

Release Availability

We strive to deliver high-quality products, and to ensure quality and seamless transitions, we roll out our products in phases. Each rollout may take up to four weeks to accomplish and is delivered in the following phases:

- **Phase 1:** Demo, Shared SaaS UATs, and Latest Mode UATs
- **Phase 2:** Shared SaaS environments
- **Phase 3:** Latest Mode environments

Getting Ready for Major OS Releases

To prepare for the upcoming software updates from major device vendors, read through the **Getting Ready for Major OS releases** section of the Omnissa Product Documentation.

Documentation

To learn more about Workspace ONE UEM, browse Workspace ONE UEM Documentation.

Localized Content for Omnissa Docs

For details on Omnissa's localization strategy, see the KB article: Announcing Omnissa Localization Support.

Support Contact Information

To receive support, access Omnissa Customer Connect. For information about filing a Support Request in Customer Connect and using Cloud Services Portal, see the KB article here.