VMware Workspace ONE UEM™ Powered by AirWatch 2203 Release Notes

VMware Workspace ONE UEM 2203

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Workspace ONE UEM Release Notes

1

VMware Workspace ONE UEM Release Notes provide information on the new features and improvements in each release. This page includes a summary of the new features introduced in 2203 and resolved issues and known issues.

When can I expect the latest version?

2

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

Once our phased rollout is complete, we will announce general availability for on-premises and managed hosted customers. For more information, see the KB article.

Getting Ready for Apple Fall 2021 Releases

3

Learn more about the upcoming Fall 2021 releases for Apple. See Getting Ready for Apple Fall 2021 Releases for more information.

New Features in this Release

4

Console

- **Locate your VMware Workspace ONE Intelligence instance more easily in the Workspace ONE Cloud Admin Hub.**

  The right navigation panel in the Workspace ONE Cloud Admin Hub now lets you to quickly locate your Workspace ONE Intelligence instance if you use Workspace ONE UEM and Workspace ONE Intelligence. Utilize the navigation menu to access your VMware Cloud Services (the square in the top right corner). To access the Workspace ONE Intelligence console, navigate to **My Services** and click the clearly labelled **Workspace ONE Intelligence Enabled**.

- **Introducing a new notification banner for smart group OG restrictions.**

  The notification banner will keep you informed of any changes to smart group OG restrictions. When you navigate to **Assignment Groups**>**List View**, you are now greeted with the following notification:*Creation of Smart Groups above Customer OGs will not be allowed in future releases*.

- **The text "Registered" on the Device and Monitor dashboard is now read as "Pre-enrollment Registration Record."**

  The number next to the text "Registered" misled users, as it refers to the registration record created on the console rather than the actual enrolled device in the registered mode of Enrollment. Therefore, we renamed "Registered" to "Pre-enrollment Registration Record" to avoid any ambiguity.

Android

- **Want to reset the work passcode while the Work Profile is locked in direct boot? We can assist you.**

  When a Work Profile is locked in direct boot, the Work Profile lock screen now prompts the user with the **Forgot my Password** button for Android 11 devices with a separate device and work profile password. For more information, see Android Device Management with Workspace ONE UEM.

Apple

- **Get notified when your Apple Business Manager tokens are about to expire.**

Admins in Workspace ONE UEM can now be notified by email or directly in the console 30 days before the expiration of an Apple Business Manager (ABM) app token or device token. Device tokens will also be able to notify admins when errors occur, such as the acceptance of new ABM Terms of Use. For more information, see Configure Console Notifications.

Application Management

- **Override the default device reboot behaviour for your win32 apps during installation.**

  Workspace ONE UEM now provides you the flexibility to define the device reboot behaviour not just at the app configuration level but also at the app assignment level. You can set the device restart options by activating the newly introduced **Override Reboot Handling** setting at the app assignment level. The restart options you configure at the assignment level override the options configured at the app configuration level. For more information, see Upload and Configure Win32 Files for Software Distribution and Add Assignments and Exclusions to your Applications.

- **Track and report app installation status on Windows devices with accuracy.**

  Workspace ONE UEM console now allows you to see the accurate installation status of applications on Windows devices. This enhancement aids in determining whether the user uninstalls the application manually. It also improves the user experience by displaying an accurate list of installed apps on the user's devices.

Content Management

- **Tweak the Acknowledge button to suit your company needs.**

  You can configure the text that appears on the acknowledgement button and the time it takes for users to acknowledge a required document. To do so, navigate to **Settings** < **Workspace ONE Content App** < **Document Acknowledgement** and enable the **Document Acknowledgement** feature. For more information see the section, Document Acknowledgment in Workspace ONE Content.

Chrome OS

- **Are you concerned about the security of user data if a device is lost or stolen? We have come up with a solution for you.**

  We've updated the management commands to include a Clear User Profiles command which logs out and deletes all users from the device. For more information, see Device Management Commands for Chrome OS.

- **You can no longer view the data that remains on your devices following an enterprise wipe.**

  We've updated the Enterprise Wipe command for Chrome OS devices with a new option to ensure all stored data is deleted after deprovisioning. We've also added a **Device Wipe** command for clearing data without deprovisioning the device. For more information, see Device Management Commands.

MacOS

- **We have enhanced the support for device Lock functionality**.

  Starting with macOS 10.14 and later devices, admins can lock a device with Apple Silicon by a six-digit PIN and can provide a message that is displayed on the unlock screen. For more information, see Lock Devices.

- **We've added support for macOS Recovery Lock**

  Starting from macOS 11.5, as an MDM administrator, you can set a password that must be entered before a user can restart an Apple Silicon macOS device into the recovery OS via API. The password can be set or removed only by the MDM solution. You can also view the recovery lock status in Event Logs. To know more, see Recovery Lock Status.

- **Microsoft conditional access support to macOS platform is now available**

  Admins can now use Azure Identity provider to authenticate access to Microsoft Office applications in the production environments. It is based on the device's compliance and management state sent to Azure from UEM for improved security posture (Unified Endpoint Management).

Rugged

- **Product delivery to devices in a SaaS environment just got easier!**

  To optimise performance and free up significant resources in UEM, use CDN to deliver products to devices. By default, we have set the provisioning setting for the organisation group that hosts devices to **Enabled**. You can check the **Product Downloads Through CDN** setting by navigating to **Groups & Settings > All Settings > Admin > Product Provisioning**.

Resolved Issues

5

Read the following topics next:

2203 Resolved Issues

- **CRSVC-27266: Unable to delete device from UEM console**
- **CRSVC-29793: S/MIME certificates seemingly corrupted on DB**
- **CRSVC-29031: UEM Unenrollment Does Not Send Re-Authentication to User's Other Devices.**
- **AGGL-11954: Apps do not appear in the Managed Google Play Store on Android Enterprise devices due to exception in the SyncAFWAppsForOwner stored procedure.**
- **AGGL-11954: setAvailableProductSet EMM API calls and App Syncs failing due to SQL exception - violation of PRIMARY KEY constraint.**
- **ARES-20866: Android Enterprise - Failed to send managed app config.**
- **CMCM-189443: Unable to Delete Managed Content through API if the file is downloaded on device.**
- **AMST-35577: Spaceman error while navigating to Devices > Lifecycle > Staging > Windows.**
- **AMST-35577: Spaceman error while navigating to Devices > Lifecycle > Staging > Windows.**
- **FCA-200853: Angular pages do not load unless role has minimum set of permissions.**
- **UM-7279: AdvancedLdapSyncJob Encounters Error**

- UM-7237: User Group User List failing to load due to dbo.UserGroup_SelectUserGroupMembers sproc timing out
- UM-7217: Error searching for oracleLDAP group on any Oracle environment.
- UM-7212: Cannot modify an Admin Role on Child OG.
- UM-7183: Updating EnrollmentUser LocationGroupUUID is not batched.
- UM-401: Automatic LDAP group sync skipped for customer intermittently
- SINST-175943: Run Airwatch cloud connector installer in silent mode.
- RUGG-10589: Copying the existing provisioning profile creates the profile copy under Devices > Profiles & Resources section.
- RUGG-10513: Custom Attribute XRef Batch Import Fails when using MAC Address.
- RUGG-10469: Provisioning/PoliciesViewDevices grid ‘Last Seen’ shows time 5 hours behind expected Admin time zone.
- RUGG-10368: macOS version information not visible in List View.
- RUGG-10364: Peripheral (Printer) File cannot be deleted from UEM Console.
- RUGG-10357: Unable to upload large files to the File/Actions menu.
- PPAT-10401: Internal SDK app throws Error Code:14 with Tunnel Proxy.
- MACOS-2705: SystemIntegrityProtectionEnabled is returned as false by device search API for MAC OS.
- INTEL-34748: DB upgrade failure.
- FCA-201419: Unable to save 'Edit Device' section on few devices.
- FCA-201427: UEM's API to retrieve Syslog settings is available on the API help page but does not work.
- FCA-201317: Customer is experiencing slowness in device search after upgrade to UEM version 21.09.

- FCA-201263: DEP TOU Accept button requires scrolling on iPod touch.
- FCA-201088: Unable to see IP Address in the Device reports column named "Wi-Fi IP Address".
- FCA-200942: Migration script Notification.UpdateNotificationUUID is causing failures in upgrades.
- FCA-201086: Unable to access User List tab in the UEM Console.
- FCA-200936: Console login failing for directory admin account with error "Invalid credentials".
- FCA-200930: UEM console crash while navigating to Devices > Compliance Policies > Event Log.
- FCA-200792: UEM reports fail to run with 'try again' status.
- FCA-200222: User Account Denial of Service.
- FCA-200674: Few admins were unable to assign already published apps | New app to be published are not impacted.
- FCA-200503: SaaS Terms of Service (TOS) is not displayed properly when accessed from outside the VMware corporate network.
- FCA-199471: Compliance Policy for Cell Data Usage does not report correct status.
- ENRL-3311: Device friendly does not get updated immediately when enrolled with the device type, but gets updated with a delay.
- ENRL-3309: Console page crashes while editing Group Policies.
- ENRL-3235: Lifecycle > Enrollment Status page shows no results after searching for a value and sorting by Enrollment Status.
- CRSVC-26687: API devices/{deviceID}/commands requires customCommandModel query.
- CRSVC-26608: The Trust Service log does not output even though the log level is changed to "verbose".

- CRSVC-26579: Event Purge for partitioned DBs not using RetentionDays for partition range.
- CRSVC-26373: SQL Blocked Processes on PROD DB.
- CRSVC-26547: Unable to delete smart groups.
- CRSVC-26530: Remove redundant call to activate vIDM connector during ACC installer build process.
- CRSVC-26308: About expected behavior for modification of Application Group(AllowList).
- CRSVC-25994: Option to create message template type "Vendor Application Group Creation Notification" missing.
- CRSVC-25970: API Framework XSS validation prevents double newline characters.
- CRSVC-25866: Certificate Request Failed error while trying installing a profile with a certificate.
- CRSVC-25779: New enrollments of Boxer fail to connect to on-premises Exchange through SEG.
- CRSVC-25745: Azure AD token revoke is not triggered by enterprise wipe.
- CRSVC-25837: Error when loading Certificate List View.
- CRSVC-25654: Install Compliance profile fails to reconcile assignment when SmartGroup is modified.
- CRSVC-25535: 'Certificate Near expiration' report returns incomplete results.
- CRSVC-25279: Compliance Policies only show Message Templates defined at the same OG as the Compliance Policy.
- CRSVC-25520: Subject line of email notification is not displaying the Umlaut (Ä ä Ü ü Ö ö) characters correctly.
- CRSVC-25200: Uptime DB Upgrade Failed.

- CMSVC-15994: Special Characters such as &&...<> are allowed when creating Smart Group via REST API.
- CMSVC-15915: Unable to find the smart groups in the WS one hub services during assignment against templates.
- CMCM-189509: Unable to access device details page for all Android devices.
- CMEM-186566: Devices are getting blocked when turning on DX Mod.
- CMCM-189498: Uploading large PDF files will cause the Web Console to become inaccessible.
- ARES-21600: DeviceProfile_SearchByDeviceDashboard_V3 causing tempdb contention.
- ARES-21597: Unable to load or edit profiles assigned to a deleted OG.
- ARES-21167: Install application commands are not generated for Public Android apps when 50 or more devices are selected.
- ARES-21063: Denylist or Non-Allowlist Application Details By Device report gives details of the devices that are not selected as a part of the Device Model.
- ARES-21025: View devices page gives empty results.
- ARES-20845: App Sync does not reconcile Internal applications for Shared devices.
- ARES-20841: Internal app publish fails due to duplicate key inserted error.
- AMST-35172: Huge number of timeouts in interrogator.windowsinformationsample_save SP
- AMST-35069: Newly enrolled Windows 10 devices install x86 version of AppDeploymentAgent.
- AMST-35070: DM & HUB having race condition causing enrollment issues.
- AMST-35043: Encryption Type always switch back to TKIP for Windows Desktop WiFi Profile
- AMST-34911: Script and Sensor Role permissions.

- AMST-34661: Removal command targets incorrectly when the app is deleted from UEM
- AMST-34554: DS cluster under stress due to ApproveUpdate windows commands.
- AMST-34527: Windows Desktop Firewall Profile does not allow editing of IP ranges after saving profile
- AGGL-11340: Spaceman error while launching Android DDUI profiles.
- AGGL-11354: Launcher Wallpaper Image Persists on Device after Removal from Design Screen
- AGGL-11353: Application details are not loading on Launcher layout configuration page.
- AGGL-11278: Approved SIM details do not get updated on the latest UEM console.
- AGGL-11352: Launcher Administrative Passcode.
- AGGL-11277: Devices not reporting feedback.
- AGGL-11275: Page crashes when editing Launcher profile with Miscellaneous app added to pinned row.
- AGGL-11265: Chrome OS Application control profile issues.
- AGGL-11242: Rocket man error when we add app for existing launcher profile.
- AGGL-11200: Custom script to add model Samsung SM-G781B.
- AGGL-11065: Android profiles cannot be viewed.
- AGGL-11142: Agent settings for gps sample interval is saving and displaying data incorrectly.
- AGGL-11135: Launcher orientation is set to locked in XML when its not selected in the UI
- AGGL-11064: Error while saving new or existing permission profile for android.
- AGGL-10992: Devices not reporting feedback from App Feedback Channel.

- AGGL-10916: Model of Android devices are missing on the console and displayed as "Android" instead.
- AGGL-11014: Permissions payload with certain applications generates invalid XM.
- AGGL-11012: Launcher profile configuration seems to be reverting to the older value when making any edits on the profile.
- AGGL-10904: DDUI Android Launcher profile cannot modify assignments without adding version
- AGGL-10901: 'Lock Orientation' checkbox gets disabled upon save.
- AGGL-10867: Unable to save value as unselected.
- AGGL-8173: Catalog shows incorrect version when Prod and Beta tracks exist.
- AGGL-10750: No Certificate batching when external CA (PKI) is used for Tunnel.
- AAPP-13345: Copying iOS Restrictions Profiles with Hide Apps payloads does not add the Hide Apps payload to new profile.
- AAPP-13333: Classroom not showing updated classes.
- AAPP-13336: Issues Removing Apple Education Profile from iPads.
- AAPP-13298: Find device option not populating when device is turned off and then on
- AAPP-13326: App Tunnel configuration is lost after changing 'Prevent Removal' setting in restrictions of app assignment.
- AAPP-13281: Home Screen Layout search results display duplicate entries.
- AAPP-13246: VPP Auto Update not working for some applications
- AAPP-13194: Derived Credentials profiles not auto installing when a new version is added.
- AAPP-13104: Unable to view assigned VPP applications from the catalog after editing the device details.
- AAPP-13149: Issue with Hiding iOS Apps on iOS 14.

- **AAPP-13169: macOS DEP enrolled devices not installing Intelligent Hub when Custom Enrollment is Enabled.**
- **AAPP-13088: Error while saving the friendly name settings.**
- **AAPP-13022: App sync failing during check in/check out.**
- **AAPP-13058: Unable to delete supervised iOS device from Device List View if enrollment status is Wipe Initiated.**
- **AAPP-13052: Bundle IDs in Hide Apps section of the Restriction profile is empty after upgrade.**
- **AAPP-13049: Migration script failed.**
- **AAPP-11166: API/mdm/devices/Search api does not show correct value for EnrolledViaDEP.**
- AAPP-12298: VPP store URL on vpp distribution page is pointing to old https://vpp.itunes.apple.com.

Patch Resolved Issues

6

Read the following topics next:

22.3.0.2

- **CRSVC-28447: ZDT upgrades making the environment inaccessible during the upgrade.**
- **AGGL-11669: Chrome OS Device Profile - Kiosk - Managed Guest Session - App not sent down.**
- **AMST-35785: Fix SOR client's base url in device services.**
- **CRSVC-28101: Add intermediate certs to chain.**

- AGGL-11654: Chrome URLWhitelist or URLBlacklist does not work on the latest Chrome Versions.

22.3.0.3

- Issue AMST-35903: Domain join fails when Smart Groups evaluated before enrollment.

22.3.0.4

- CRSVC-28397: Migration of few devices failing due to missing compliance_status value.
- AMST-35882: Unable to run Selective App list API call on the certain enrolled Win 10 devices.
- MACOS-2701: Add patch.sql to execute DeviceQueue_MigrateSeededMacOsProfileMacOs2629.
- AMST-35753: Windows OS build version shows different in device List View and device Summary page.
- CRSVC-28931: Unable to install S/MIME profile due to a "certificate is used more than once error."
- AGGL-11680: DDUI is broken by a certificate date format in Android profiles.
- CRSVC-28385: Page fail for ADCS CA in aa.

22.3.0.5

- AMST-35867: Seed v2203.3 patch Hub to UEM.
- CMSVC-16129: Tags update API fails when organization Group ID is not passed.
- FCA-202719: Unable to delete devices from UEM console.
- AMST-35971: Unable to update internal app assignments for some Windows applications.
- UEM unenrollment does not send re-authentication to other user devices.

- UM-7449: Admin Groups not updating after Automatic or Manual Sync.
- CRSVC-28588: GSX certification save failed with password invalid.
- AMST-35916: Blobs being served by Device Services even when they are present in the CDN and StorageType is set to 1.
- AMST-35879: Windows Application Deployment Commands are only cleared after a manual Query or App Sample Query from UEM console.

22.3.0.6

- CRSVC-27265: Message Template notification type is not considered while sending token related email.
- AAPP-13822: VPP licenses are not getting disassociated.
- AMST-35969: Dropship Provisioning-Device Registrations never make it to through the Bulk Importer Service.
- CMEM-186613: Delay in adding the device to the allow list from email list view.

22.3.0.7

- AGGL-11954: Apps do not appear in the Managed Google Play Store on Android Enterprise devices due to exception in the SyncAFWAppsForOwner stored procedure.
- AMST-36098: Seed the v2203 Patch SFD to UEM.
- UM-7478: Devices unable to move to different Organization Group based on UserGroup Mappings after Auto Sync.
- AMST-36007: Greater Than or Equal to application detection operator not working.
- AGGL-11900: Handsfree R5 devices are listed incorrectly in DB and the UEM.
- INTEL-38869: Intelligence - Recovery Key Escrowed value not matching UEM.
- CRSVC-29264: Time Windows not accessible.

- AAPP-13877: MDM profile errors out with "Decryption key for the profile is not installed".

22.3.0.8

- CRSVC-28863: Async email notifications cause thread pool exhaustion and suspends compliance evaluation.
- AGGL-11973: Zebra device model being reported as Unknown.

22.3.0.9

- PPAT-10981: Clicking on "Manage Tunnel Access" optionin the console crashes the page.
- AMST-36175: Customer cannot upload missing dependencies for some .appx files while editing them.
- CRSVC-29618: Failed to view device summarytroubleshooting in UEM console 2203 when admin locale set to Chinese.
- FCA-202994: Device wipe initiated for devices even if admin cancels the request mid-way.

22.3.0.11

- AAPP-14003 Username not visible in the tvOS "Wi-Fi" payload.
- AGGL-12047: Model of Android devices are missing on the console and displayed as "Unknown" instead - script correction.
- ARES-22163: Slide Forced and Idle session timeout for blob upload use case.
- CRSVC-29793: S/MIME certificates seemingly corrupted on DB.
- FCA-203016: Unauthorized endpoint in MVC > Angular migration: Account > Administrators > System Activity > Batch Status.
- MACOS-3173: Add support for Mac Studio set of devices in the UEM console.

- UM-7478: Devices unable to move to different Organization Groups based on UserGroup Mappings after Auto Sync.

22.3.0.14

- AMST-36290: Disable HardwareDeviceIdentifierForWindowsFeatureFlag.
- CRSVC-29626: Triggering the 5K API calls per minute limit even though ithas been longer than a minute

22.3.0.15

- AMST-36328: Seed the v2203 Patch SFD to UEM console.
- AMST-36335: UEM Azure AD integration button ink is broken.
- PPAT-11097: Error while publishing the gateway notification on compliance status change.

22.3.0.16

- AGGL-12139: Android Chrome Browser profile fails to save URL Blocks & Exceptions.
- AAPP-14121: [Device State] Enrollment exception for device POST calls with missing compliance status.
- AGGL-12218: Compliance Enterprise Wipe should factory reset device.
- PPAT-11696: Windows tunnel client "Not Configured" and certificate getting revoked with Reason Code: Superseded.
- CRSVC-30280: Include device state supplemental tools config files in UpdateSQLServerInfo tool.

22.3.0.17

- CRSVC-30607: Layout issue in connected date field for localized content.

- **CRSVC-30609: The translated strings "connected" and "Deauthorize" are not loaded in Google BeyondCorp card.**
- **CRSVC-30611: The connected date is not localized.**
- **AMST-36418: EnrollmentToken Purge encounters FK error.**
- **CMCM-189868: Intelligence | Sandbox ETL logs ingestion very high.**
- **FCA-203340: Sending query to device results in multiple device query requested events in troubleshooting event logs for device.**

22.3.0.18

- AGGL-12273: Delay in device checking post console upgrade from v21.1.0.23 to v22.3.0.15 causing product to be in queued state unless device is queried/synced.
- AMST-36560: ACC and AWCM times out while publishing content to Adaptiva.
- CRSVC-30604: Integrated Authentication certificate does not rotate to new CA when we modify the settings for the Web under SDK settings.
- CRSVC-30902: Email (SMTP) test connection fails but the console can send emails.

22.3.0.19

- CRSVC-30895: Unable to delete Certificate Authority.
- FS-1423: Workflows are getting stuck at blocked and do not proceed.
- MACOS-3278: Seed the Model information for new "M2" Macs.
- INTEL-41600: ZDT DB upgrade failed while deleting SP and type.
- CRSVC-31184: Entitlement service migration tool fails to connect to database on DB credential change.

22.3.0.20

- ENRL-3520: Add Token Preview behind a Feature Flag.
- FCA-203721: Device export with xlsx format with wrong display model.
- AMST-36752: App deployment options not retained on Save & Publish.
- RUGG-11302: Product provisioning is not getting assigned post upgrade.
- AMST-36624: Seed v2203.4 Hub to UEM Console.
- CRSVC-31344: DSM action cleanup stored procedure throws collation error when the server and database collation is different.

22.3.0.23

- AAPP-14462: Delay in OS seed script deployment is causing data inconsistency.
- AGGL-12338: DDUI profiles cannot be created or edited.
- CMCM-190024: DB Server CPU spiking to 100% multiple times a day.

22.3.0.24

- CRSVC-31784: GSX test connection fails with SSL error.
- AMST-36839: Device context based applications require valid user session to process uninstall.
- ARES-22791: Mac Studio Assignment update missing/unselected.

22.3.0.25

- MACOS-3334: Device Details page crashing for Linux devices when loading processor architecture from latest Device State Service.
- FCA-203857: Unable to load Angular Exports page.

- FCA-203818: Improve performance of API_LoadDevice.
- ENRL-3533: Unenrollment date is Null in Intelligence.
- AMST-36974: Unable to edit app assignments.
- PPAT-12130: Change the Tunnel Devices API from Public to Internal API.

22.3.0.26

- FCA-203863: Unable to edit Device Asset number.
- AGGL-12887: URL Blocks & Exceptions in Chrome Browser Profile disappeared with data loss (upgrade from 2102 to 2203).
- AGGL-12899: Time mentioned in System Updates profile changes to AM from PM after save and publish when UI Locale languages is Japanese, Chinese, or Korean.

22.3.0.28

- AMST-36830: Windows Firewall Rule not working as intended on Win 10 device.
- AGGL-12934: Group Organization Mode change command not queued after changing to Fixed Organization Group.
- CRSVC-32059: “Renew Certificate" not working as expected in Certificate list view.
- AMST-37025: SSL Pinning showing not synchronized.
- CMEM-186702: PowerShell failing: "User credential of the remote PowerShell server contains the special characters."

22.3.0.29

- CRSVC-31980: Unable to publish scripts due to errors with console.
- CRSVC-32318: Add telemetry for counting usages of the unsigned Secure Channel payloads.

22.3.0.30

- AGGL-13123: Fix the incorrect Model being updated for a device from system samples - Zebra devices are being reported as model type "unknown" in Smartgroup filter.
- CRSVC-32528: Compliance status is pending and "next compliance check" date is in the past.

22.3.0.31

- AGGL-13171: setAvailableProductSet EMM API call fails due to SQL truncation Error.
- AMST-37306: Since upgrading 22.4.0.12 (2204) Custom profiles are not installing for newly enrolled Windows devices.
- AMST-37333: Compromised status change for Mac Devices are flooding Event Logs table.
- CMSVC-16562: Assignment page crashing intermittently for Internal Applications.

22.3.0.32

- AAPP-14775: Cannot Enable Device Assignment for certain VPP applications.
- AMST-37437: Sensors Tab on Device Detail View should be visible for Registered Mode devices.
- FS-1887: Unable to edit freestyle orchestrator workflow with Time Window condition.

22.3.0.33

- INTEL-42458: Managed Application List Initial Export creation
- CMCM-190216: Intermediate SQL timeout exception seen on test environment.
- CMCM-190183: Unable to delete content from List view or through API (500 error).
- AMST-37311: Device Identifier & UDID mismatch for any reason should not unenroll device.

22.3.0.34

- AGGL-13298: Saving profiles containing encrypted string fails due to Enum mismatch.
- AGGL-13299: DDUI - Request to increase maximum character limit for fields in Chrome Browser settings profile.
- RUGG-11545: Smartgroups with OS version criteria not updating when a device updates OS version.

22.3.0.35

- AAPP-15009: Remove Custom Server Certification Validation and include the new Apple Root Certificate as part of the installer.
- AGGL-13425: DDUI - Request to increase the maximum character limit for fields in the Chrome Browser settings profile.
- AMST-37557: Security sample improvements.

22.3.0.36

- AMST-37744: (P2P Branch-Cache) Peer to Peer download is not working.
- ARES-23911: Terms of Use page crashes in console.

22.3.0.37

- AAPP-15139: Certain VPP Apps are stuck Pending Check.
- CRSVC-34143: Add debug logging to the HMAC Canonical code.
- CMSVC-16660: Unable to delete Smart Groups.

22.3.0.38

- FS-2453: FS-1887 changes did not make it to Astro Air.

22.3.0.39

- FS-2332: Unable to delete Internal applications.
- AMST-38004: Unable to modify and save the install command for Windows app.

22.3.0.40

- MACOS-3567: macOS - add support for new hardware released.
- AMST-38165: Location option missing in Bulk management for Windows devices.

22.3.0.41

- AGGL-13810: Microsoft Surface Duo (Android) enrollment is blocked even though Microsoft as Manufacturer is allowed.
- PPAT-13434: iOS VPN Profiles have the incorrect DTR ruleset getting applied for devices.

22.3.0.42

- RUGG-11791: Policy Engine stuck on environments without processing items in queue.
- AMST-38263: Improve products delivery for newly enrolled devices.

22.3.0.43

- AAPP-15489: Beacon sample should trigger Device Info sample but should not save OS data.
- AMST-38338: Antivirus and Firewall status are periodically failing.

22.3.0.44

- CRSVC-35972: Refactor EventLogService to use concurrent bag.
- INTEL-47437: Windows devices getting unenrolled.

22.3.0.45

- MACOS-3664: Decouple code changes to seed new MAC models.
- RUGG-11907: Dollar($) character is removed from Allowlist specific Android activities on reopening the profile.

22.3.0.46

- ARES-24851: Add additional logs on the File upload and Purge utility delete functionalities.
- ENRL-3705: Beacon flow is wrongly updating OS info.

22.3.0.47

- PPAT-14132: After migration to AWS CloudFront, Tunnel Configuration page does not load.
- CRSVC-36381: Sample handling issue not going back to the correct time.
- AAPP-15872: Phase 1 of Rapid Security Response support.

22.3.0.48

- AAPP-15992: Renewed VPP stoken(ASM) does not sync the app details on the console.

22.3.0.50

- SINST-176153: Updated Code signing certificate.

22.3.0.51

- SINST-176173: DDUI Profile Screen Fix.

22.3.0.52

- SINST-176199: Update Installer to fix issues with DDUI profile screen.

22.3.0.53

- SINST-176173: Fixed issues with DDUI profile screen.
- CMEM-186886: PowerShell script and Workspca eONE UEM side changes for EXO V3 module.
- AGGL-15441: Unable to create Android profile with a TimeSchedule, whose ScheduleListUUID is Null.
- CRSVC-40042: Only save public key component of certificate to database.
- AGGL-15324: Remove EFOTA sample from microservices.
- PPAT-14514: .NET core version upgrade to 6 for Tunnel microservice.
- CRSVC-39362: Memcached uses only one server.
- CRSVC-40107: Private key not exportable in manual flow.
- CRSVC-37822: Migrate invalidate refresh token flow from AAD to Microsoft graph API.
- CRSVC-37515: Update token refresh Azure AD graph API call.

22.3.0.54

- AAPP-16437: Update Device Information query Cellular keys.
- CMCM-190723: Status of document in content detail report was not corrected.
- MACOS-4057: macOS 14 ADE enrollment fails if Custom Enrollment is off.
- AGGL-15527: Google seems to have increased oAuthToken length (AndroidWorkSetting AccessToken got truncated).

Known Issues 7

Read the following topics next:

Launcher

- **AGGL-11106: Adding a version to Launcher profile inside a product causes Launcher to stay on reload screen.**

  When a Launcher profile is deployed through Products, it is updated with a new version. The profile is removed and reinstalled which leaves the device in reload state until the new version is installed.

  As a workaround, you can deploy the new version of Lauuncher through Profiles & Resources and not through updating the Provisioning profile.

Console

- **CRSVC-28284: Version comparison returns false if there is discrepancy in the decimal placement.**

  For File & App conditions in Workflows, if a user does not provide all the decimal places for version field, the condition may be reported as Condition not met.

  There are no workarounds for this issue.

- **FS-1003: Donut Chart and Device List displaying inaccurate data.**

  On Workflow details page, the donut chart displaying the total number of impacted devices and the list of devices does not filter data by Organization Group and workflow version. So, the counts and list of devices on a parent or child OG level, are same. Also, the data does not consider the workflow version for which these details are currently displayed.

  There is no current workaround for count of devices. The device list can be identified by looking at the impacted devices by Organization Group level under Device menu.

- **FS-1005: Freestyle Orchestrator workflow identifier version is showing up in string format instead of the friendly version identifier.**

  Workflow identifier version on Intelligent Hub is displayed as a string format instead of an end user friendly format. This might lead to bad UI experience for end users but does not impact the functionality of workflows.

  There are no workarounds for this issue.

- **FS-1006: Unsupported profiles are accessible in the workflow search.**

  The unsupported profiles like Disk Encryption and Software Update hybrid profiles for MAC are searchable in Workflows profile search. If these profiles are used, the workflows can be stuck in 'In-progress' state.

  There are no workarounds for this issue.

- **HUBW-7131: Apps installing outside the assigned Time windows.**

  If multiple Freestyle workflows each installing one to two apps are using Time windows, the apps may get installed outside the Time windows.

  You can install multiple apps in a single workflow.

- **AMST-35367: Unable to delete users with removable storage associated with account and no way to remove association**

  UEM User Delete fails when Removable Drive encryption is associated with the user.

  No known workaround.

- **UM-7415: Devices unable to move to different Organization Groups based on UserGroup Mappings after Auto Sync.**

  When User Group Membership changes happen on AD which is greater than 3000, the Auto Sync updates the membership on the console and DB, however some of the users with changed User Group Membership fail to move to different OG's as per User Group Directory Mappings.

  Use API to correct the mapping.

  There is an API which can help you to move a device to an OG:

  https://\ {env}/api/help/#Unable to render embedded object: File (/apis/10002?) not found./CommandsV1/CommandsV1_ChangeOrganizationGroupAsync*replace {env} with environment nameAPI request:/devices/{id}/commands/changeorganizationgroup/{organizationgroupid}

- **ENRL-3396: Admin is able to override enrolled enrollment token records.**

  Device registration records already consumed by enrolling devices can be updated to denylist/allowlist records via UI or via batch import by uploading an excel sheet.

  If we have to convert the consumed token to Allow Device type, then the consumed token must be deleted and the fresh Allow Device record should be added.