Release Notes

December 2019

What's New

This month we're introducing two new features: Android Kiosk Mode and Device Pre-Enrollment. Kiosk Mode is a security feature that allows an admin to lock down a device so activity is limited to a specific app or task. The new Device Pre-Enrollment feature lets an admin set up targeted configurations in advance to be automatically deployed during enrollment.

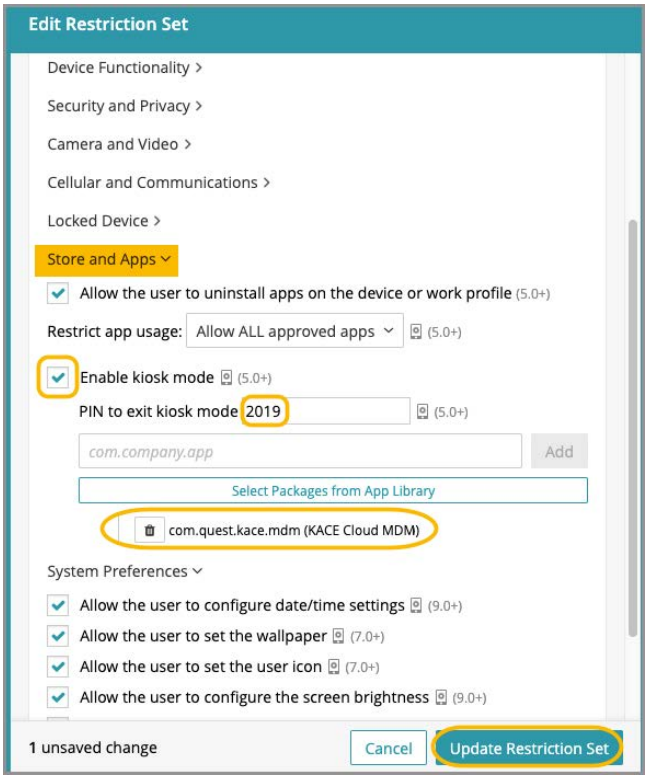
We're also adding multi-server capabilities for our existing DEP/Zero-Touch Enrollment feature and additional functionality to our existing Android App Usage Restrictions.

New Features:

Android Kiosk Mode

Kiosk Mode is a security feature that allows an admin to lock down a device so activity is limited to a specific app or task. For example, if a sales team uses certain devices exclusively for giving demos of their product, their admin can enable kiosk mode to run the specific demo software on those devices and nothing else.

From the library, kiosk mode can be applied to an existing set of restrictions or when adding a new restriction set. An admin enables kiosk mode then selects packages from the app library that can be used on the device(s). A PIN can also be created that will allow a device to temporarily exit kiosk mode. This is a useful function if an admin ever needs to temporarily exit kiosk mode—for example, if a Wi-Fi configuration is no longer valid and they need to manually add a new one to regain connectivity.

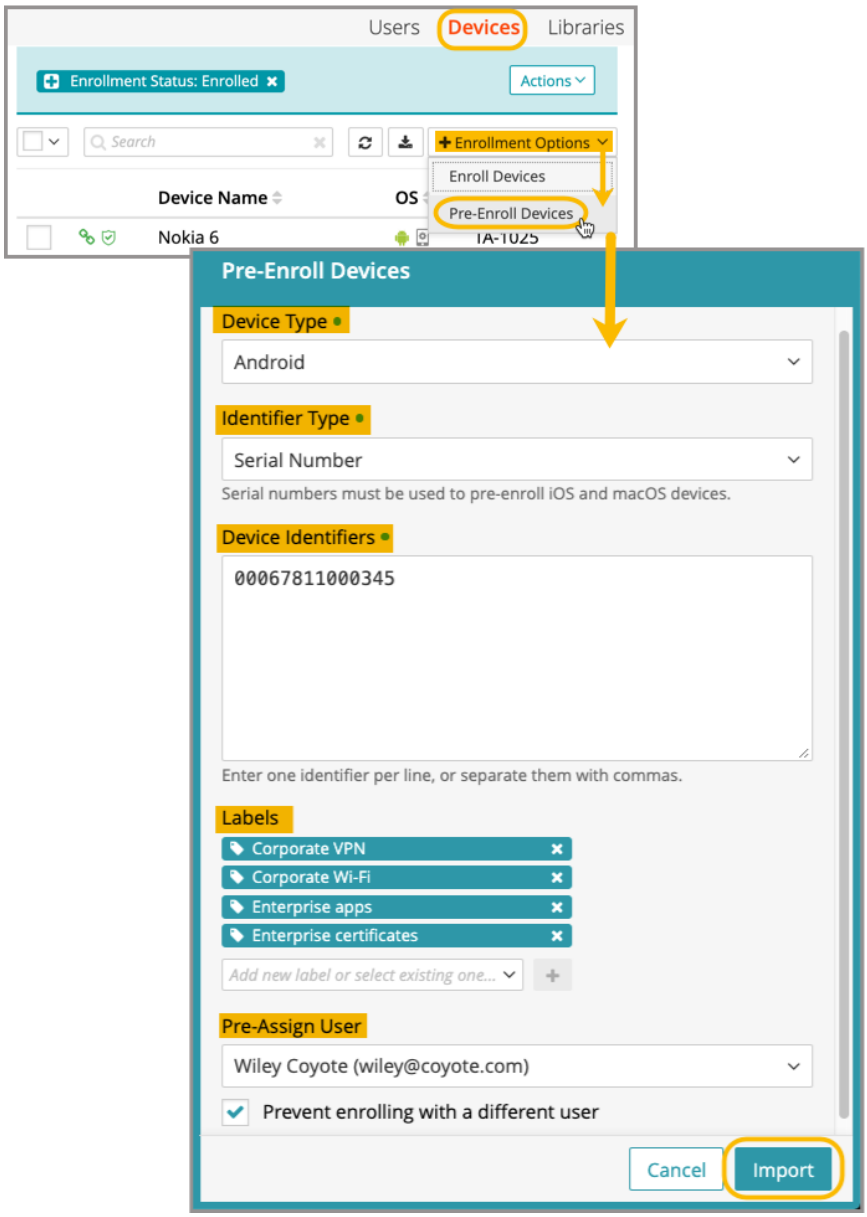


Learn more about Android Kiosk Mode.

Device Pre-Enrollment

The new Device Pre-Enrollment feature lets an admin set up targeted configurations in advance to be automatically deployed during enrollment.

From the Devices section, an admin can choose to complete pre-enrollment by accessing Enrollment Options > Pre-Enroll Devices. The pre-enrollment form lets an admin enter device types, identifier types, device identifiers, and add manual labels that will cause any associated policies to automatically deploy rules, restrictions, and other configurations at the time of enrollment. Note that if the pre-enrolled device matches any smart label, configurations from policies associated with that label will be deployed during enrollment. An admin also has the option to pre-assign users to devices during pre-enrollment.



Learn more about Device Pre-Enrollment.

Feature Enhancements:

DEP Multi-Server Capabilities

Our DEP Zero-Touch Enrollment feature enhancement lets an admin sync multiple DEP accounts with a single tenant. When an admin syncs multiple virtual MDM servers within DEP, it allows them to set a default DEP profile for each device type (iPhone, iPad, macOS, tvOS, iPod). Note that the default device types for each virtual MDM server are set within Apple Business Manager or Apple School Manager, and a default DEP profile can be set for each DEP enrollment.

Learn more about DEP Multi-Server Capabilities.

Android - App Usage Restrictions

Basic usage restrictions for Android are currently available in the form of 'Allow ALL approved apps' and 'Allow specific apps'. With this release, we've added the choice to 'Block specific apps'.

The ability to block specific apps is especially helpful when an admin needs to approve a broad set of applications across an enterprise, but also needs to allow a small subset of users to access specific apps exclusively—for example, a marketing team that requires access to Facebook and Twitter. Blocking apps can also serve as a security feature if an admin needs to immediately disable a specific app in the case of a vulnerability.

Learn more about Android App Usage Restrictions.

Resolved Issues

Issue	Description	Status
3576 - Adding a user to a manual label associated with a policy does not update policy	When a user was associated with a manual label, policies were not being reevaluated.	Fixed
3575 - Wrong user account used during re-enroll if user was deleted and recreated	If a user was deleted and recreated, the deleted account was being used during device enrollment instead of the new user account.	Fixed
3572 - Unenrolled and deleted device gets marked as enrolled on next inventory	If an Android device was unenrolled from KACE Cloud and deleted before the agent had a chance to process the command, the device would get added back to the inventory as "enrolled" the next time the agent checked in.	Fixed
3563 - App package picker in Android Restrictions shows iOS apps	The screen for selecting apps from the app library was showing iOS when editing an Android restriction set.	Fixed
3556 - Initiating user for unenroll commands is not tracked	The user that sent the unenroll command to the device was not being tracked in the device history screen.	Fixed
3555 - VPP synchronization to apple only updates apps in the US store	KACE Cloud was only retrieving data from the US Apple app store when synchronizing apps linked through the Volume Purchase Program.	Fixed
3554 - Managed app configuration viewport is too small	Buttons were being pushed off the screen when editing a managed app configuration if the browser window was too small.	Fixed
3551 - DEP Sync is clearing the asset tag field	The asset tag field was being overwritten by the asset tag found in the Apple device record during a DEP device sync. The sync process now only sets the asset tag field if it is empty.	Fixed
3548 - VPN library config doesn't allow a colon	A port number could not be specified in the server name field of a VPN configuration because the field did not allow a colon.	Fixed
3541 - Suspend tracking switch is available even though the admin selects to never allow tracking suspension	If the admin configured the location rule set to never allow tracking suspension, the "Suspend Tracking" switch was still visible in the KACE Connect app.	Fixed
3534 - Update app store import to clarify free vs paid apps	The help text on the import screen of the app library indicated that only free apps were supported. The text was updated to let admins know that paid apps could be purchased through Apple Volume Purchase Program (VPP) or the Google Managed Play Store.	Fixed
3532 - App Library picker in restrictions shows app entries for each app configuration	When selecting an app in a restrictions set, the app list included apps with all the various configurations that had been created for it instead of only showing the app name itself.	Fixed
3528 - Unable to create Android Zero Touch Profiles	Some customers were receiving an error code 400 when attempting to create a Zero Touch profile through the KACE Cloud MDM portal.	Fixed
3515 - UI: Cancel edit of ZTE or DEP profile puts UI in useless state	When cancelling out of editing a Google Zero Touch profile or an Apple DEP profile, the UI could get stuck in a unusable state, requiring a browser window refresh.	Fixed
3419 - Notification shows "UPDATE_APP" in text	The notification for updating an app was not showing the correct text after a managed configuration was modified.	Fixed
3414 - Multiple "Default settings" configs created after VPP sync	When apps were synchronized from the Apple Volume Purchase Program, a new "Default settings" configuration was being created, even if one already existed.	Fixed
3361 - Enrolling an iPad running iPadOS displays wrong message after initial profile	When enrolling an iPad running iPadOS 13+, the end user was not being instructed to go to the Settings app to complete the enrollment.	Fixed
2876 - Need DEP sync button to do full re-sync	The Sync button on the Apple Device Enrollment Program screen only performed an incremental sync instead of a full sync, which could lead to device counts getting out of sync.	Fixed

Known Issues

Issue	Description	Status
3514 - iOS update command does not display status feedback.	iOS command to update OS uses default action that will typically download but not install. Fix to display status feedback.	Open
3286 - Apparent mismatch between device compliance and individual entity compliance.	Occasionally the policy details for a device may show success even if the entity in question did not successfully install.	Open
3108 - Auto-deployed Android restrictions don't appear in the device restrictions list	If auto-deployed restrictions for Android are sent to the device, the database may not be properly updated.	Open
3070 - System attempts to remove policy configs when unassigned device is assigned to a user	During reassignment of a device to a user, removal of previous configurations may fail. If this happens, it may be possible to work around this by first unenrolling the device.	Open
Android - Role Management and SSO Configuration	If user role assignment is set to Automatic during SSO Configuration, a manual attempt to update an individual user's role via the Users > Edit User path may appear possible, but will be overwritten by the original SSO Configuration. To resolve, the configuration setting can be changed to Manual, which will then enable editing of individual user roles.	Open
Android - Restrictions	Restrictions that are configured to deploy upon enrollment may not immediately appear in the inventory for impacted devices; however, the restrictions will be enforced on the device.	Open
Android - Device Owner Setup	When using the Device Owner enrollment flow (afw#kace), the enrollment flow may not complete if the Google Play services on the factory default image of the device are out of date. This a known issue with the Android operating system, caused by the enrollment process timing out before the update of the Play Services on the device can complete. You will know that this situation occurred if you are never asked for your subdomain name during the enrollment process. If you end up back at the device home screen, locate and launch the KACE Cloud MDM agent app on the device and click the 'Enroll Device' button to complete the setup process.	Open
Android - Gmail App	Android devices require the Gmail app to be installed in order to use the email account configurations.	Open
Android - Set and Clear Passcode Commands	The set and clear passcode functions are different in Android 7.0 and later. On versions prior to 7.0, an administrator could set or clear the passcode as desired. On Android 7.0 and later, the passcode can only be set on devices that do not already have a passcode set, and passcodes cannot be cleared. The user interface does not currently warn users who are attempting to set or clear a passcode on Android 7.0 and later, but an error message will appear. Note that attempting to clear a passcode will also fail if there is a policy in place that requires use of a passcode to do so.	Open
iOS - Factory Reset: Apple iOS iCloud Account Lock	When resetting an Apple iOS device back to factory defaults, the device will remain locked to the associated iCloud account. To prevent this from happening, before resetting the device, manually turn off the 'Find my phone' feature on the iPhone.	Open
macOS - macOS 10.15 Account Configuration	During enrollment, if the 'Prevent Primary Account Changes' option is checked and DEP authentication is enabled, the primary account will be created automatically using the DEP authentication token as the account password. While still in the enrollment process, the password cannot be changed. However, once enrollment is complete, the account password can be changed as normal.	Open

Additional Resources

Getting Started Guide

Admin Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA
92656

Refer to our website (www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal.

Trademarks