Release Notes

October 2017

What's New

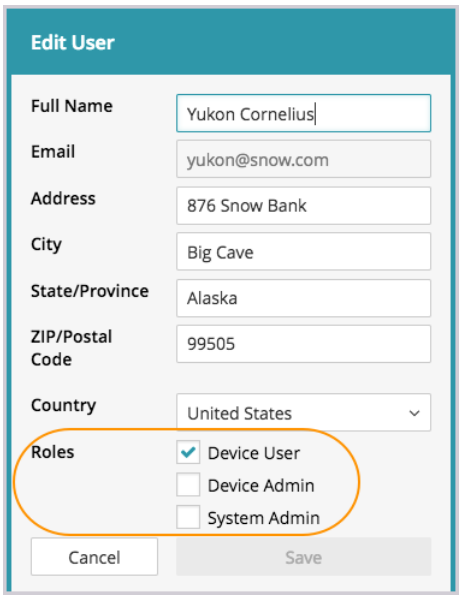
New Feature: Enrollment Restrictions

The October 2017 update of KACE® Cloud Mobile Device Manager introduces the ability for device administrators to control which users can enroll a device. This builds on the improved role management features added in the previous release.

Currently, a user can be assigned one or more of three roles, as described in the table below. With this release, there is a new rule that affects the Device User: A user **must be** assigned the Device User role to successfully complete enrollment in KACE Cloud MDM.

Role	Privileges
Device User	• Can enroll their own device. Note: A user must be assigned the Device User role to successfully complete enrollment.
Device Admin	• Can view, add, modify, and delete users. • Can view the roles that are assigned to device users. • Can assign/unassign the device user role. • Can view and send commands to all devices.
System Admin	• Can view, add, modify, and delete users. • Can assign/unassign roles for device users, device admins, and system admins. • Can view and modify SSO configurations and SMA Integration settings. • Can map LDAP groups.

An Admin can confirm a specific user's role assignments using the Edit User function.



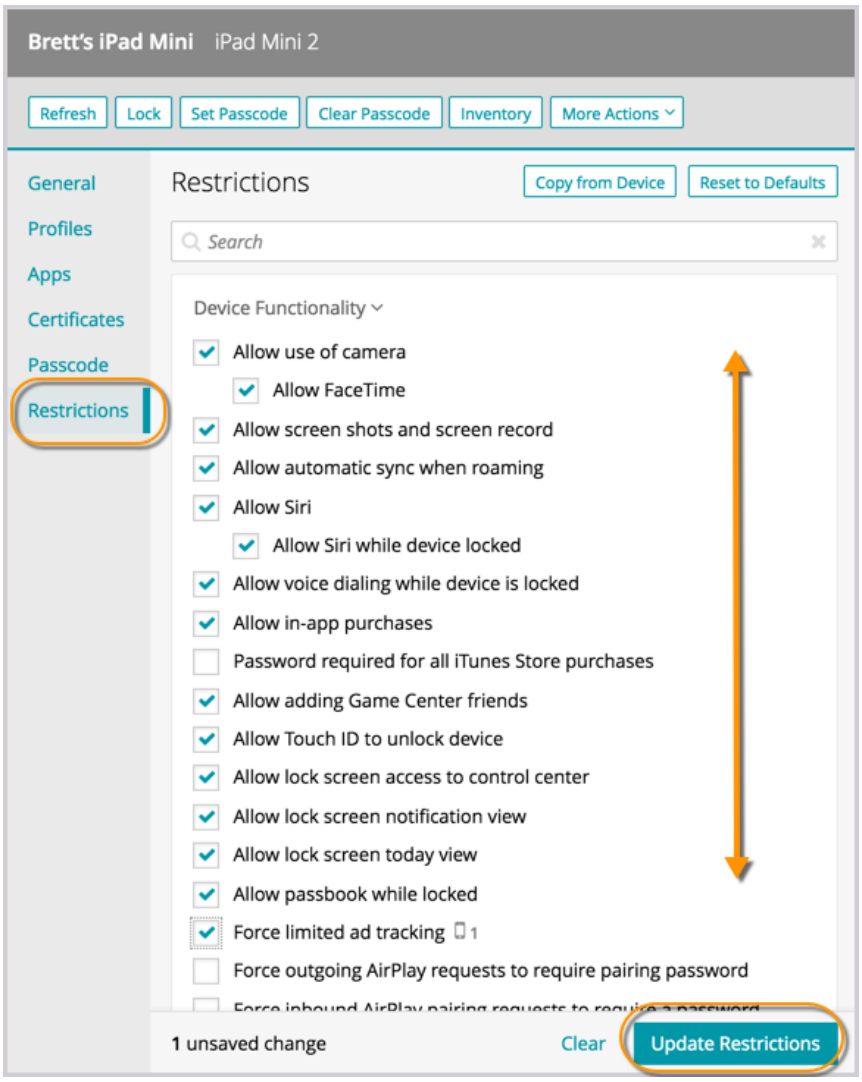
The Device User role can also be assigned automatically through Single-Sign-On (SSO) configuration settings.

New Feature: Device Restrictions

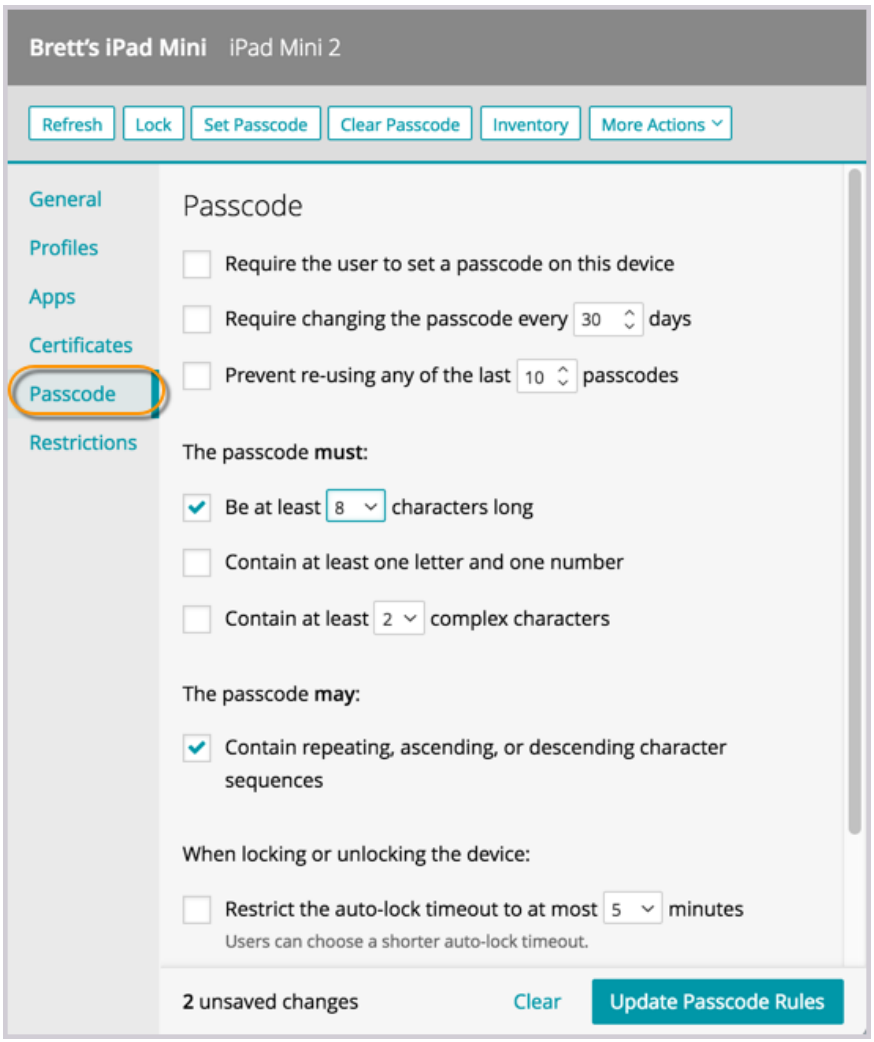
Device Administrators can now set passcodes, lock screens, and set camera restrictions on both iOS and Android devices. In addition, iOS devices have a variety of general, security, application, App Store, and content rating restrictions.

Restrictions are currently configured on a per-device basis, but profile-based configuration of devices will be available in the near future.

An Admin can set or clear restrictions by choosing a user, then making updates in the Restrictions section.

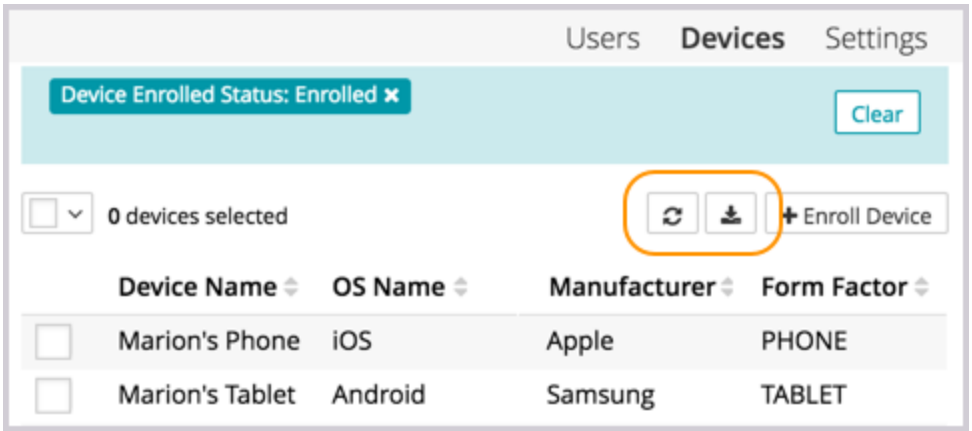


In addition, Admins now have access to a comprehensive list of passcode restrictions in the Passcode section.



Enhancements: Refresh and Export Device List

Two new functions are located at the top of the device list: Refresh and Export device list.



Refresh

The Refresh button refreshes the devices list without refreshing the entire browser, and without losing selected filters.

Export Device List

A CSV file export includes all of the public device attributes stored in KACE Cloud MDM, not just those visible in the list. The list does not include any child list data, such as applications, certificates, profiles, or restrictions, but it does include all hardware attributes.

Known Issues

Account Linking

If you manually create an account in KACE Cloud MDM, then use SSO to log in using the same email address, your account will be automatically linked to single sign-on. You will receive a confirmation email so you can verify.

Android - Set Passcode Command

The Set Passcode function changed in Android N and later. On versions before N, an administrator could set the passcode as desired. On Android N and later, the passcode can only be set on devices that do not already have a passcode set. The user interface does not currently warn users who are attempting to set a passcode on Android N or later.

Expired Password Links

Password reset links are valid for 65 minutes. If you click a password reset link that has expired, you will receive a generic message indicating that there is a problem. Click the link included with the message to be taken back to your main login page, then click the "Forgot Your Password?" link to reset your password.

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.

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

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.