Release Notes

January 2018

Feature and Functionality Recap

In our initial product launch, KACE Cloud Mobile Device Manager was introduced with the following features:

- User Management
- Device Management
- Filtering
- Alerts and Notifications
- Single Sign-On Support
- KACE Systems Management Appliance (SMA/K1000) Integration

Product enhancements over the past 6 months have included:

- Device Ownership Designation
- Advanced Filtering Capabilities
- Improved Role Management
- Enrollment Restrictions
- Device Restriction Management
- Data Export Capabilities
- Library Management
- Certificate and Wi-Fi Management

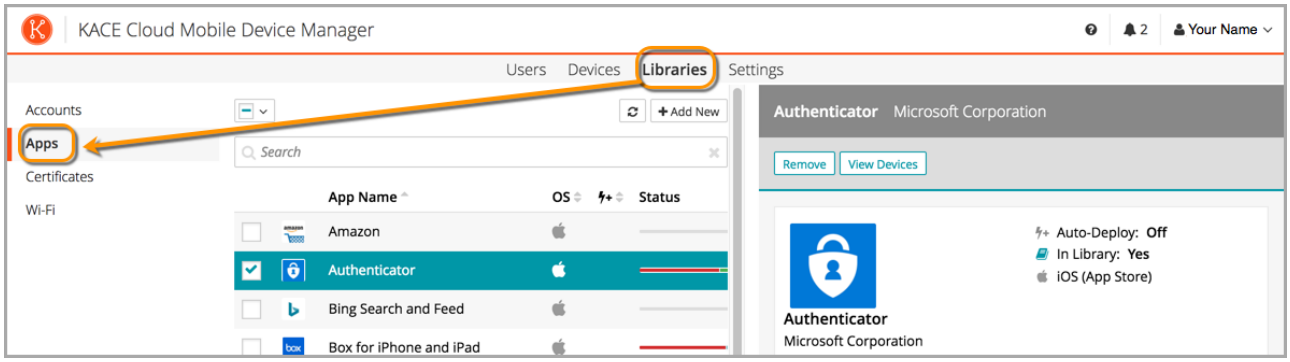
What's New

Our January 2018 release provides administrators with two new device management features: App Management for iOS and Account Management. With App Management for iOS, device administrators can manage and push both free App Store apps as well as custom apps (i.e., enterprise apps) to iOS devices. And with Account Management, device administrators can create and push account profiles to both iOS and Android devices.

New Feature: Application Management for iOS

Apps can be added to devices via library, local machine, or app store. Functionality includes the ability to add and remove apps on individual or multiple devices—including the ability to view all devices with a specific app installed, as well as view only KACE-managed apps on a device or devices.

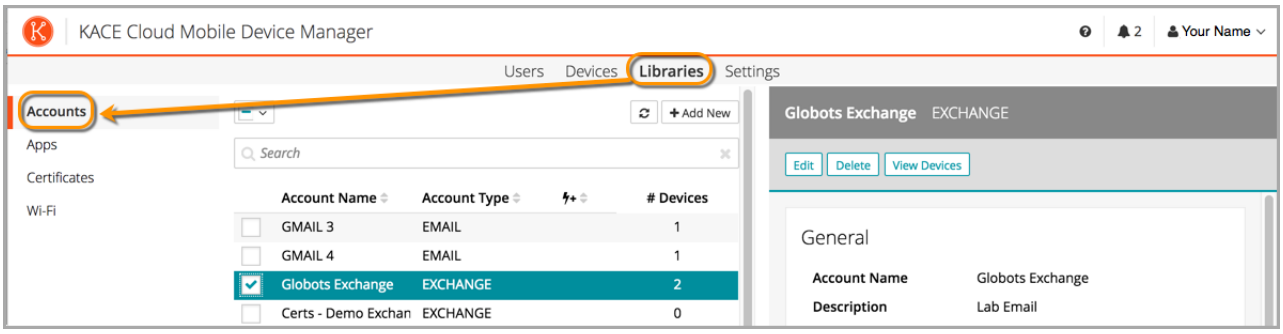
App management for Android is not currently supported.



New Feature: Account Management

Account configurations can be added to devices via library or manual set-up using supported email account types, including Exchange ActiveSync and Gmail (iOS and Android) and POP3/IMAP (iOS). Functionality includes the ability to add new account configurations directly to the library or devices, edit account configurations in the library, and remove account configurations from the library or individual devices.

An account can be configured with a specific username or associated with the user's KACE Cloud MDM account. When the profile is sent to the device, the information is pulled from the user account associated with that device, enabling a single profile to support most users in the organization.



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.

Role Management and SSO Configuration

If user role assignment is set to Automatic during SSO Configuration, a manual attempt to update an individuals 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.

Android Considerations

App Updates

An end user will need to log in to the Google Play Store while in the Work Profile on their Android device in order to receive app updates. This extra step will be eliminated once App Management for Android is launched in KACE Cloud MDM.

Certificate Removal

The ability for an admin to remove a certificate is not currently available for Android devices.

Change in Android Enrollment

In order to receive account profiles on an Android device, the KACE Cloud MDM agent app will need to be updated to the latest version available in the Google Play Store, and the device will need to be re-enrolled. This should be a one-time re-enrollment process that will allow the agent app to create a Work Profile on the device.

Gmail App

Android devices require the Gmail app to be installed in order to use the email account configurations.

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.

iOS Considerations

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.