KACE® Cloud Mobile Device Manager v1.0

Release Notes

July 24, 2017 - v1.0

What's New

Introducing KACE® Cloud Mobile Device Manager (KACE Cloud MDM)—a new SaaS solution that makes it easy to manage and inventory all of the mobile devices that access your network. With KACE Cloud MDM, you can:

- Protect your network from mobile security threats while providing visibility and management of mobile devices on your network.
- Enroll, inventory, and manage mobile devices on the most common platforms.
- Collect inventory, manage passwords, erase, and easily reset mobile devices.

Learn more about KACE Cloud MDM.

Features

User Management

- Create, edit, and remove user accounts
- Designate which accounts are administrators
- View devices associated with an account

Device Management

- Enroll and unenroll Android and iOS devices
- Retrieve inventory information about enrolled devices
- Lock devices to prevent unauthorized access
- Set passcodes on device to prevent unauthorized access
- Clear a passcode from a device (on supported platforms) to unlock and allow access to device
- Reset devices to their factory settings
- Send commands to multiple devices simultaneously

List Filtering

- Filter the user list by user attributes
- Filter the device list by device attributes
- Filter the user list by device attributes, allowing you to see which users have devices meeting the specified filter criteria
- Filter the device list by user attributes, allowing you to see which devices are associated with users meeting the specified filter criteria

Alerts

- Receive real-time alerts in the product to track the status of commands as they execute
- Directly navigate from the alert to the user or device by clicking the name of the user or the name of the device
- Clear old notifications

Single Sign-On Support

- Integrate KACE Cloud MDM with any SAMLv2 or OpenID Connect identity provider to provide single-sign-on with company account credentials
- Map security groups to the administrator group to enable easy management access

KACE Systems Management Appliance (SMA/K1000) Integration

- See all your systems inventory in a single pane of glass by synchronizing your KACE Cloud MDM device inventory into the KACE SMA
- Synchronization does not consume any additional licenses on the SMA
- Set up a recurring discovery schedule on the KACE SMA
- KACE SMA 7.2+ is required for integration with KACE MDM

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, KACE Cloud MDM will prompt you to link those two accounts together. In the future, this prompt will be removed and the accounts will automatically be linked, but for now, you will need to accept the prompt to link the accounts. You will still be able to log in using both the SSO-linked account that uses your company account credentials and with the KACE Cloud MDM account that uses the password you set initially.

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. If you receive this message, go to the main login page for your subscription (the link is provided in your "Welcome" email) and click the "Forgot Password?" link. A new email message will be sent to the email address you provide allowing you to choose a new 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.

SSO Account Lockout

There is a possibility that an account could be locked out if the user account role mapping is not set up correctly. To avoid this situation, we recommend that admins create a backup user account using a personal email address and designate it as an administrator. This will ensure that an admin can still access the system in the event that their work account is locked out. This issue will be resolved in the next release. In the meantime, if you do experience an accidental account lockout, please contact support for assistance. We will create a support account in your subscription and help you work through the SSO configuration issues.

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.