

# Release Notes

August 2017

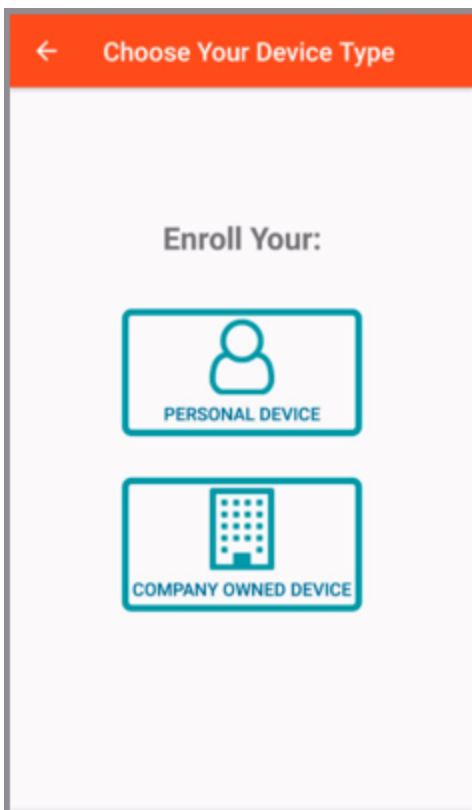
## What's New

### New Feature: Device Ownership Designation

The August 2017 update of KACE® Cloud Mobile Device Manager introduces the ability to designate whether a device is company-owned or personal (i.e., BYOD). This is a foundational attribute that will allow device administrators to differentiate how devices are managed in their environments.

#### Enrollment Changes

During the device enrollment process, the device user will be given the option to specify who owns the device—whether it's company-owned or personal. The process is the same for both iOS and Android devices, but the option shows up in different places. For iOS, the device user is given the option in their enrollment portal [<https://mycompany.enroll.kacecloud.com/>] immediately after they log in. For Android, the device user is given the option after they click Enroll Device in the [Android agent app](#). Below is an example of the screen in the Android agent app:



#### Administrator Override

The device administrator has the option to override the user-specified value by selecting the device in the Devices list, then changing the device ownership attribute in the device detail pane, as shown below. A company device can also have an asset tag specified. Note that once enrolled, a device user will be unable to change this setting without unenrolling and re-enrolling their device.

Please set the device ownership.

Unknown  
 Personal Device  
 Company Device

Asset Tag

### Filtering the Device List

Device administrators can now filter the device list based on the device ownership attribute and/or the asset tag (for company-owned devices). If a bulk factory reset command is issued against a list of devices that contain both company and personal devices, only the company devices will be reset.

**Ownership**

Company  
 Personal  
 Unknown

### Restrictions on Personal Devices

In this release, the Factory Reset command is prohibited for personal devices. All new features that are released in the future will take into account the difference between personal and company devices.

### Update Notes

All currently enrolled devices have been designated as Personal. As mentioned above, a device administrator can change this value in the device detail panel if desired.

## Enhancement: Improved Role Management

In the August 2017 update, we are introducing a new role, renaming two roles, and changing the way roles are managed.

### New Role: System Administrator

We are introducing a new system administrator role and redefining the existing administrator role as device administrator. Any user with the system administrator role will be able to modify system settings, such as Single Sign-on (SSO) and KACE Systems Management Appliance (SMA) integration. The system administrator is also allowed to manage users and assign roles to other users.

The system administrator role cannot be automatically assigned through SSO user role mapping, but the device administrator and device user role can be. This resolves the user account lock-out issue noted in the [original release notes](#)—it is now impossible to lock out any system administrator due to incorrect SSO user role mappings.

### Device Administrator Role

The existing administrator role has been renamed as device administrator, and will have a more focused set of permissions relating to only device and user management. Users with this role will no longer be able to change SSO or SMA integration settings, but they will retain their ability to manage user accounts and devices. Any user account created by a device administrator is automatically granted the device user role.

### Device User Role

The existing user role has been renamed as device user. The device user role is a baseline permission granted to all users who have enrolled a device. System administrators and device administrators are automatically granted the device user role.

<b>Roles</b>	Device User Device Admin System Admin
--------------	---

### Integrated Role Management

The original role management screen under Settings has been eliminated, and the functionality has been merged into the existing Edit User screen, as shown below:

The screenshot shows the 'Edit User' form with the following fields and values:

- Full Name: Jason H
- Email: Jason@email.com
- Address: 100 Candy St.
- City: Cambridge
- State/Province: OH
- Zip/Postal Code: 10013
- Country: United States
- Roles:
  - User
  - Device Admin
  - System Admin

Buttons: Cancel, Save

### Upgrade Notes

All accounts with the former administrator role have been automatically granted the new system administrator role, so there will be no change in current capabilities for existing users.

## 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. 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](#)

---

© 2017 Quest Software Inc.

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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](http://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](http://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](http://www.quest.com/legal). All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.