Release Notes

November 2019

What's New

In our November release, we're introducing Location Tracking as a new feature in KACE Cloud MDM. Location tracking lets administrators monitor and maintain their device inventory with functions that allow them to:

- Enable or disable the location tracking feature
- Collect real-time location information
- Set range for collecting data location
- Enable or disable device suspend limits
- Set compliance parameters
- Link or display the company's data privacy policy, and
- Provide a complete location history of device(s)

Note: Location tracking is available for iOS and Android devices, but is not currently available for Mac devices.

In addition to location tracking capabilities, we've added two feature enhancements. For device list exports, username and email columns have been added to the .csv file. For Android app installations, the default has been reset so that unknown sources will be allowed to install apps on Android devices.

New Feature: Location Tracking

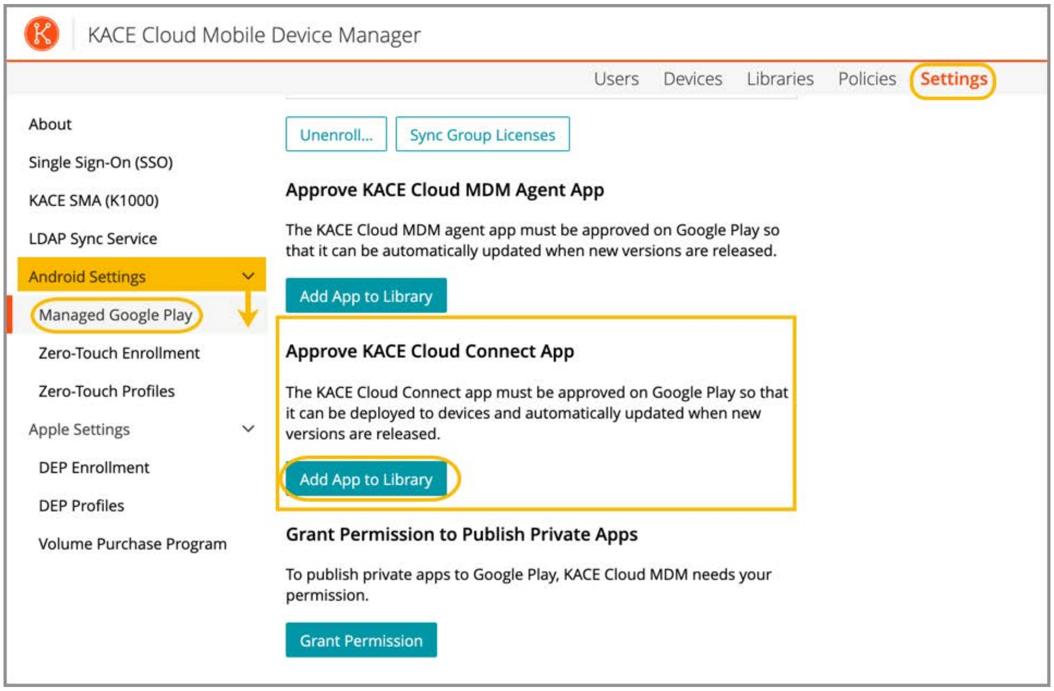
To create a unique location tracking configuration, an admin will add a new rule set. To deploy that rule set to a specific group of users or devices, an admin can link the rule set to an existing policy. Like Restriction Sets and Passcode Rules, Location Rules can be accessed through the Libraries.

Approve KACE Cloud Connect App (Android)

To successfully deploy the KACE Cloud Connect app to Android end users, an admin will first need to add the app to KACE Cloud MDM. (The KACE Cloud Connect app is automatically imported into the library for iOS.)

1. Go to **Settings** in top navigation.
2. Select **Android Settings** in left navigation.
3. Select **Managed Google Play**.
4. Under 'Approve KACE Cloud Connect App', click **Add App to Library**.

(Reference image on next page.)



Approve KACE Cloud MDM Agent App

The KACE Cloud MDM agent app must be approved on Google Play so that it can be automatically updated when new versions are released.

Approve KACE Cloud Connect App

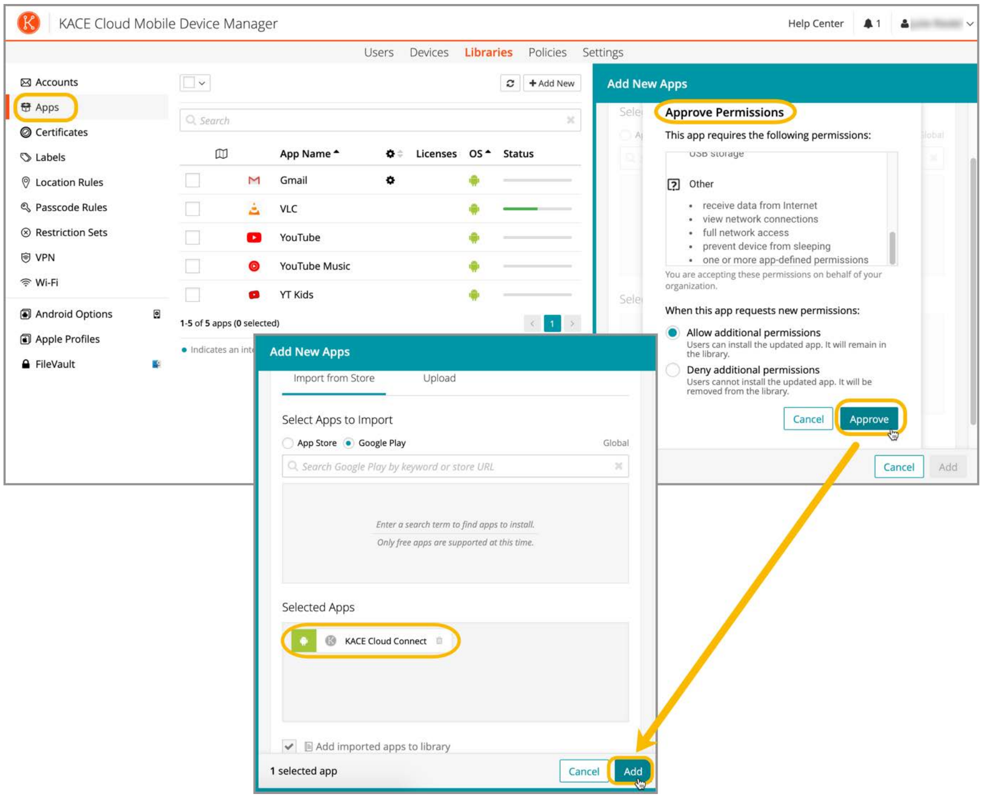
The KACE Cloud Connect app must be approved on Google Play so that it can be deployed to devices and automatically updated when new versions are released.

Grant Permission to Publish Private Apps

To publish private apps to Google Play, KACE Cloud MDM needs your permission.

The admin will be taken to the **App Libraries page** to complete the process.

1. In the right panel, review/update permissions, then click **Approve**.
2. To add the app to the library, click **Add**.



App Name	Licenses	OS	Status
Gmail			
VLC			
YouTube			
YouTube Music			
YT Kids			

1-5 of 5 apps (0 selected)

Add New Apps

Approve Permissions

This app requires the following permissions:

USB storage

Other

- receive data from Internet
- view network connections
- full network access
- prevent device from sleeping
- one or more app-defined permissions

You are accepting these permissions on behalf of your organization.

When this app requests new permissions:

● Allow additional permissions
Users can install the updated app. It will remain in the library.

○ Deny additional permissions
Users cannot install the updated app. It will be removed from the library.

Add New Apps

Select Apps to Import

○ App Store ● Google Play Global

Search Google Play by keyword or store URL

Enter a search term to find apps to install.

Only free apps are supported at this time.

Selected Apps

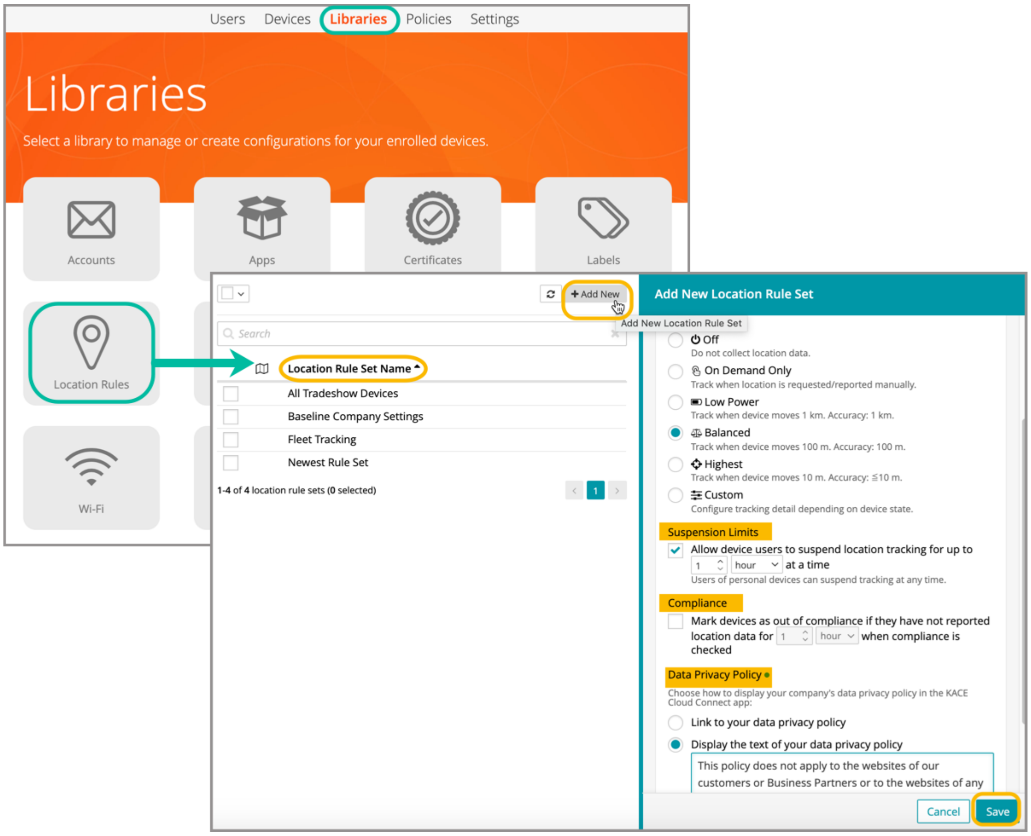
KACE Cloud Connect

☑ Add imported apps to library

1 selected app

Add a New Location Rule Set

1. Go to **Libraries** in top navigation.
2. Select **Location Rules**.
3. Click **Add New**.
    - Make selections to configure the rule set.
4. Click **Save**.



Select a library to manage or create configurations for your enrolled devices.

	Location Rule Set Name
□	All Tradeshow Devices
□	Baseline Company Settings
□	Fleet Tracking
□	Newest Rule Set

1-4 of 4 location rule sets (0 selected)

Add New Location Rule Set

○ Off
Do not collect location data.

○ On Demand Only
Track when location is requested/reported manually.

○ Low Power
Track when device moves 1 km. Accuracy: 1 km.

● Balanced
Track when device moves 100 m. Accuracy: 100 m.

○ Highest
Track when device moves 10 m. Accuracy: ≤10 m.

○ Custom
Configure tracking detail depending on device state.

Suspension Limits

☑ Allow device users to suspend location tracking for up to 1 hour at a time
Users of personal devices can suspend tracking at any time.

Compliance

□ Mark devices as out of compliance if they have not reported location data for 1 hour when compliance is checked

Data Privacy Policy

Choose how to display your company's data privacy policy in the KACE Cloud Connect app:

○ Link to your data privacy policy

● Display the text of your data privacy policy

This policy does not apply to the websites of our customers or Business Partners or to the websites of any

The 'Add New Location Rule Set' Form

Name - Mandatory. The parameters of rule sets can vary greatly, so it's important to create a distinct and utilitarian name for each.

Description - Optional but recommended. Depending on the size of your organization and the variety of rule sets you create, it is always helpful to create a record of why the rule is being created and listing any special notes that could easily be forgotten.

Detail Level - The detail level allows an admin to decide whether or not to enable data collection. And if enabled, whether to capture data in an on-demand capacity; regulate itself when the device is on low power; set a balanced limit; set the highest possible tracking levels, or to create a custom configuration for tracking detail.

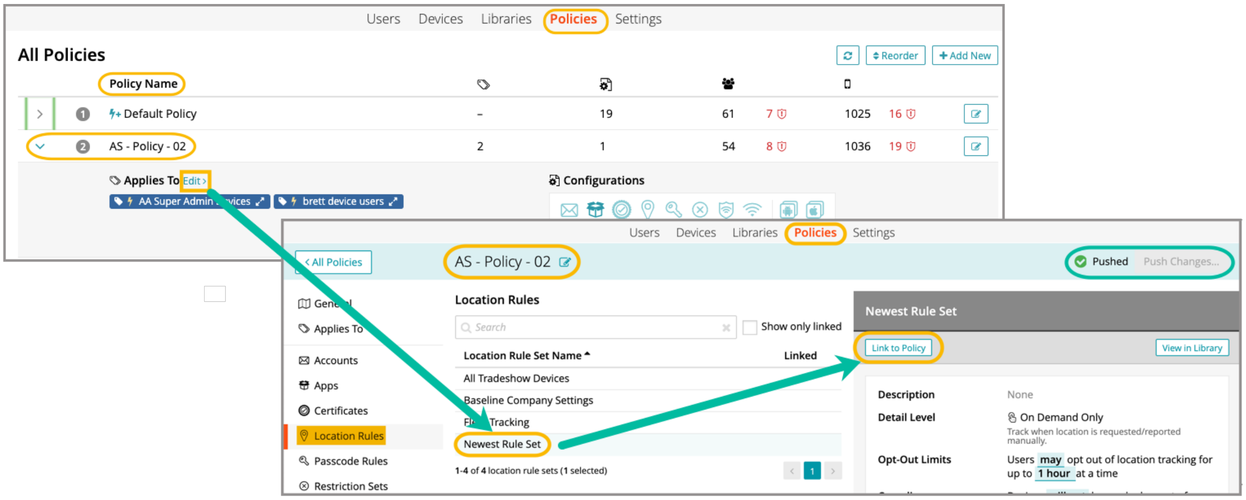
Compliance - The compliance setting lets an admin mark devices as out of compliance if they have not reported a data location for a set amount of time (hours or days) when compliance is checked.

Data Privacy Policy - An admin can choose how to display the company's data privacy policy to an end user, either through a link to the policy that will open a new window, or by pasting the full text of their policy into the KACE Cloud MDM form to display within the workflow.

Add Location Rules to Devices or Groups of Devices

To link rules to users and devices, use Policies.

1. Go to the **Policies section** in top navigation.
   - Select and existing policy.
2. Next to the **Applies to** section, click **Edit**.
3. Select **Location Rules** in the left-hand panel.
   - Select the rule set you'd like to link to the policy.
4. Click **Link to Policy**, then click **Push Changes**.



All Policies

	Policy Name							
1	Default Policy	–	19	61	7	1025	16	
2	AS - Policy - 02	2	1	54	8	1036	19	

Applies To Edit >

AA Super Admin vices · brett device users

AS - Policy - 02

Location Rules

□ Show only linked

Location Rule Set Name	Linked
All Tradeshow Devices	
Baseline Company Settings	
Fl Tracking	
Newest Rule Set	

1-4 of 4 location rule sets (1 selected)

Newest Rule Set

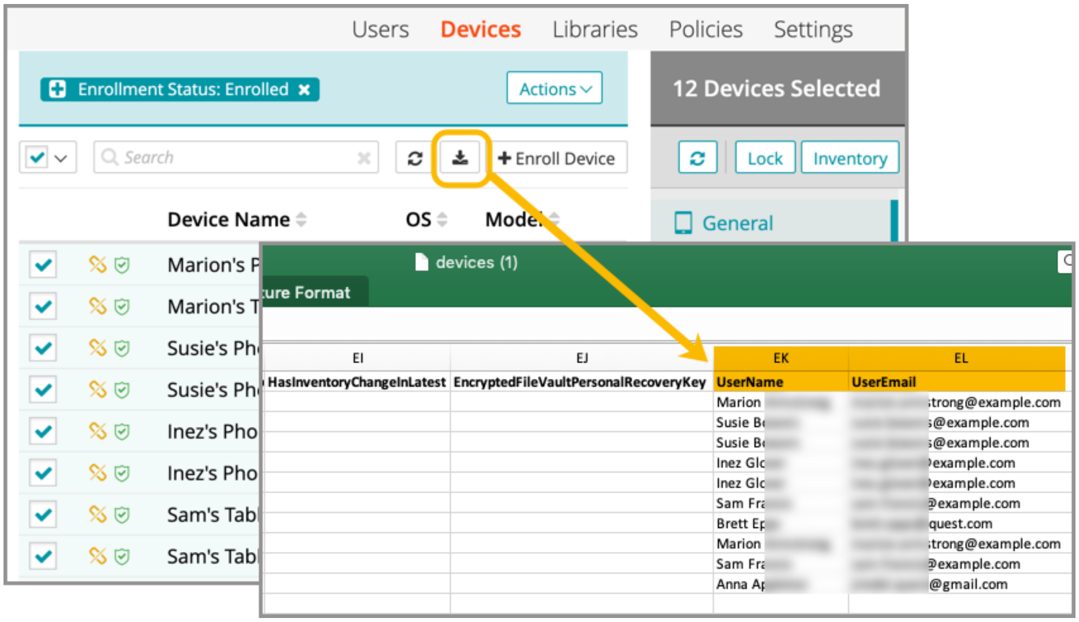
Description	None
Detail Level	On Demand Only Track when location is requested/reported manually.
Opt-Out Limits	Users may opt out of location tracking for up to 1 hour at a time

Notifying end users: Once changes have been successfully pushed, an admin will need to notify their end users that the KACE Connect app has been deployed to their devices. All end users will then need to open the app on their device and follow the prompts to allow location tracking—and for iOS, to allow notifications.

Feature Enhancements:

Device List Exports

The device list export now contains the username and email address of the user assigned to the device.

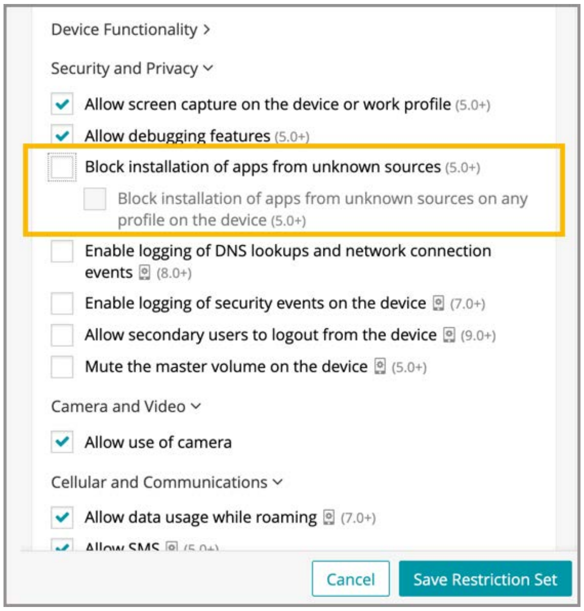


	Device Name
☑	Marion's P
☑	Marion's T
☑	Susie's Ph
☑	Susie's Ph
☑	Inez's Pho
☑	Inez's Pho
☑	Sam's Tab
☑	Sam's Tab

EI	EJ	EK	EL
HasInventoryChangeInLatest	EncryptedFileVaultPersonalRecoveryKey	UserName	UserEmail
		Marion [redacted]	[redacted]strong@example.com
		Susie B[redacted]	[redacted]s@example.com
		Susie B[redacted]	[redacted]s@example.com
		Inez Gl[redacted]	[redacted]example.com
		Inez Gl[redacted]	[redacted]example.com
		Sam Fr[redacted]	[redacted]@example.com
		Brett Ep[redacted]	[redacted]quest.com
		Marion [redacted]	[redacted]strong@example.com
		Sam Fr[redacted]	[redacted]@example.com
		Anna Ap[redacted]	[redacted]@gmail.com

Android App Installations

The default status of the 'Block installation of apps from unknown sources' restriction has been changed to allow installations from unknown sources.



Device Functionality ›

Security and Privacy ⌄

- ☑ Allow screen capture on the device or work profile (5.0+)
- ☑ Allow debugging features (5.0+)
- ☐ Block installation of apps from unknown sources (5.0+)
  - ☐ Block installation of apps from unknown sources on any profile on the device (5.0+)
- ☐ Enable logging of DNS lookups and network connection events (8.0+)
- ☐ Enable logging of security events on the device (7.0+)
- ☐ Allow secondary users to logout from the device (9.0+)
- ☐ Mute the master volume on the device (5.0+)

Camera and Video ⌄

- ☑ Allow use of camera

Cellular and Communications ⌄

- ☑ Allow data usage while roaming (7.0+)
- ☑ Allow SMS (5.0+)

For more information on location tracking and rules, please visit the Location Management section in the Help Center.

Resolved Issues

Issue	Description	Status
3524 - Username and email should be added as columns on the "Export Devices" csv report.	The username and email address that a device is assigned to should be added as columns on the existing device inventory report on the same row as the other device data.	**Fixed**
3271 - Installation from unknown sources disabled by default on Android.	Enable (add restriction to allow) app installation from unknown sources on Android devices.	**Fixed**

Known Issues

Issue	Description	Status
3528 - Unable to create Android Zero Touch Profiles	Customer received an error code 400 when attempting to create a Zero Touch profile in the portal.	**Open**
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

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) 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.