

Release Notes

December 2017

What's New

In this release, we have added a Library feature that lets device admins upload and store content for easy access and management. We are launching this feature with two libraries: Certificates and Wi-Fi. Device admins can now upload and deploy CA certificates to all managed devices as well as push and manage WEP, WPA/WPA2, and WPA/WPA2 Enterprise profiles in KACE Cloud MDM.

New Feature: Libraries

The new Libraries tab can be found in the top navigation of the product. Within this section are the Wi-Fi and Certificate libraries.

The screenshot shows the KACE Cloud Mobile Device Manager interface. The top navigation bar includes 'Users', 'Devices', 'Libraries' (highlighted with a green circle), and 'Settings'. On the left sidebar, 'Wi-Fi' and 'Certificates' are listed, with 'Wi-Fi' also highlighted by a green circle. The main content area displays a table of Wi-Fi configurations. A message on the right states 'No Wi-Fi Configuration Selected'. At the bottom, it indicates '1-13 of 13 wi-fi configurations (0 selected)'.

<input type="checkbox"/>	Wi-Fi Name	SSID	🔌	# Devices
<input type="checkbox"/>	WiFi Office 5	WiFry		0
<input type="checkbox"/>	WiFi Office 7	LAN of the Lost		0
<input type="checkbox"/>	Proxy Wifi Test	Proxy Wifi Test		0
<input type="checkbox"/>	hijkluiu80gm	vbnmy789		1
<input type="checkbox"/>	Internet Conn	doofenshmirtz-evil-corp		1
<input type="checkbox"/>	Thundercats	Thundercats-Ho! Secon		1
<input type="checkbox"/>	Wifi With Trusi	Wifi With Trusted Certif		0
<input type="checkbox"/>	Config with m	Config with multiple tru		0
<input type="checkbox"/>	Voltron	Voltron Connection 5g		1
<input type="checkbox"/>	Yichen's Cool \	SteakandEggs		0
<input type="checkbox"/>	Don blairno2	blairno2		1
<input type="checkbox"/>	Don2 blairno2	blairno2		0
<input type="checkbox"/>	Test for Trainir	wwdi-apple		1

New Feature: Certificate Management

Users can now Add and Remove certificates on single or multiple devices. New certificates can be added directly to the library at any time. During the *Devices > Certificates > Add New* process, certificates can be copied from the library or uploaded to the product.

The screenshot shows the KACE Cloud Mobile Device Manager interface. The top navigation bar includes 'Users', 'Devices', 'Libraries', and 'Settings'. The 'Libraries' section is active, and the 'Certificates' tab is selected. A search bar and a '+ Add New' button are visible. A table lists various certificate issuers, with 'COMODO Certification Authority' selected. The details panel on the right shows the certificate's validity, issuer information, purpose, and fingerprint.

Issuer	Expires On	# Devices
<input type="checkbox"/> GeoTrust Universal CA 2	3/3/2029	61
<input type="checkbox"/> QuoVadis Root CA 2 G3	1/12/2042	60
<input checked="" type="checkbox"/> COMODO Certification Authority	12/31/2029	60
<input type="checkbox"/> AddTrust External CA Root	5/30/2020	66
<input type="checkbox"/> Staat der Nederlanden Root CA	3/25/2020	60
<input type="checkbox"/> Root CA Generalitat Valenciana	7/1/2021	60
<input type="checkbox"/> Cybertrust Global Root	12/15/2021	60
<input type="checkbox"/> TWCA Global Root CA	12/31/2030	60
<input type="checkbox"/> GlobalSign	1/18/2038	57
<input type="checkbox"/> Swisscom Root CA 1	8/18/2025	60
<input type="checkbox"/> IGC/A	10/17/2020	60
<input type="checkbox"/> AddTrust Public CA Root	5/30/2020	67

COMODO Certification Authority Details:

- Unknown**
 - Valid until 12/31/2029, 5:59 PM
- Issuer:** CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
- Purpose:** The key can be used to sign a certificate revocation list (CRL). The key can be used to sign certificates.
- Fingerprint:** 0c2cd63df7806fa399ede809116b575bf87989f06518f9808c860503178baf66
- This certificate is in the certificate library

New Feature: Wi-Fi Management

Users can now Add, Edit, and Remove Wi-Fi configurations on single or multiple devices. New Wi-Fi configurations can be added directly to the library at any time. During the *Devices > Wi-Fi > Add New* process, a Wi-Fi configuration can be copied from the library or added new.

KACE Cloud Mobile Device Manager 🔍 3 👤 Your Name

Users Devices **Libraries** Settings

Wi-Fi 🔄 + Add New

Certificates

	Wi-Fi Name	SSID	📶	# Devices
<input type="checkbox"/>	WiFi Office 5	WiFi Fry		0
<input type="checkbox"/>	WiFi Office 7	LAN of the Lost		0
<input type="checkbox"/>	Proxy Wifi Test	Proxy Wifi Test		0
<input type="checkbox"/>	hijklui80gm	vbnmy789		1
<input type="checkbox"/>	Internet Connect	doofenshmirtz-evil-corp		1
<input type="checkbox"/>	Thundercats	Thundercats-Ho! Second V		1
<input checked="" type="checkbox"/>	Wifi With Trusted	Wifi With Trusted Certificat		0
<input type="checkbox"/>	Config with multi	Config with multiple truste		0
<input type="checkbox"/>	Voltron	Voltron Connection 5g		1
<input type="checkbox"/>	Yichen's Cool WIF	SteakandEggs		0
<input type="checkbox"/>	Don blairno2	blairno2		1
<input type="checkbox"/>	Don2 blairno2	blairno2		0
<input type="checkbox"/>	Test for Training	wwdi-apple		1

1-13 of 13 wi-fi configurations (1 selected) < 1 >

Wifi With Trusted Certificates Wifi With Trusted Ce...

Edit Save As... Delete

Wi-Fi > Details

General

Name	Wifi With Trusted Certific...
SSID	Wifi With Trusted Certific...
Auto-Deploy 📶	No
Auto Join	Yes
Hidden Network	No
Disable Captiv...	No

Proxy Settings

No Proxy Configured

Security Settings

Security Type	WPA2 Enterprise
Accepted EAP ...	PEAP

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 individual's 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

Certificate Removal

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

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](#)

© 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) 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.