KACE® Cloud Mobile Device Manager update

WHAT'S NEW IN KACE CLOU MOBILE DEVICE MANAGER?

Whether you are managing a bringyour-own-device (BYOD) program or keeping track of corporate-owned mobile devices, you need to be able to effectively deploy, manage and secure your mobile endpoints just as you do your traditional endpoints.

The KACE® Cloud Mobile Device Manager by Quest simplifies modern device management, so you can protect your organization's investment in Android iOS, macOS and Windows 10 devices. This helps you streamline device configuration and management — all from a single console.

When integrated with the KACE Systems Management Appliance, the KACE Clou Mobile Device Manager provides users with a comprehensive inventory of traditional and mobile devices — all visible from the KACE Systems Management Appliance dashboard. This integration gives you a unified endpoint management strategy that includes visibility and control over every device used to connect to your organization's resources.

With the latest release of the KACE Cloud Mobile Device Manager, you gain:

- **Visibility —** You can't manage and secure what you can't see. Gain full visibility into modern endpoints, including attributes and applications deployed, regardless of whether devices are corporateowned or belong to employees.
- **Security —** Secure mobile devices from outside threats, and wipe lost or stolen devices to protect corporate data. Prevent data bleed on personal devices by virtually segmenting corporate and personal data on employee-owned devices.
- **Ease of management —** Manage mobile devices from deployment to end of service. Deploy free or paid apps on Android and iOS devices that help employees do their jobs better.

NEW FEATURES

- **Microsoft Office 365 support —** Deploy Office 365 to any enrolled Windows device, as long as you have a Microsoft Office 365 subscription.
- **Apple DEP web authentication (Mac and iOS) —** Get full account authentication, including single sign on (SSO), during the Device Enrollment Program (DEP) process. This option eliminates the need for generating authentication tokens for iOS 13 and Mac 10.15 or newer devices.
- **SAML-based SSO updates —** Enable automatic checking and validation of your identity provider signatures using the Security Assertion Markup Language (SAML) to update SSO settings across your environment. This daily check can prevent authentication issues resulting from expired signatures.

For more information about KACE Cloud Mobile Device Manager, view the demo or contact sales.

Handout-KACECloudMDM-Q2-US-LP-62908