Release Notes

September 2020

What's New

In our September release, we're introducing several helpful updates, including DEP authentication; additional support for Windows 10; and enhanced automation and visibility when validating SSO certificates.

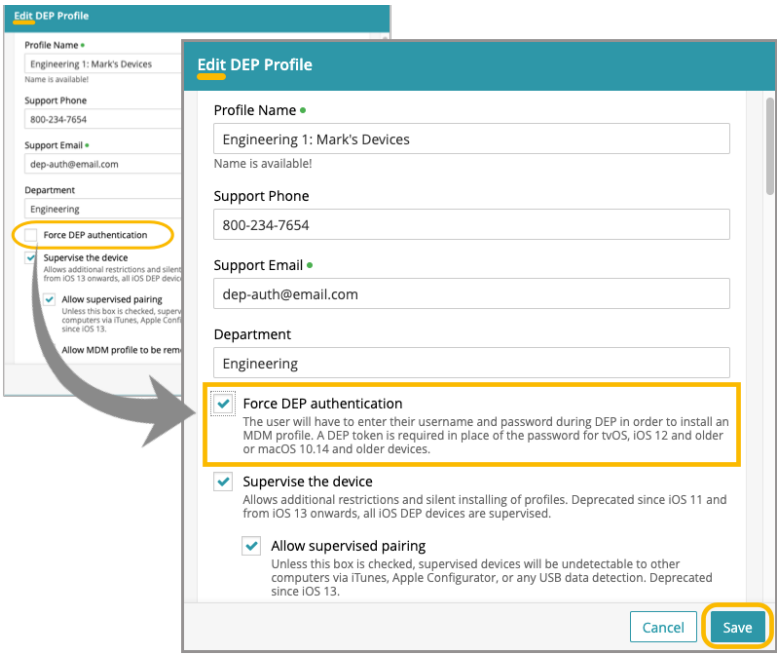
During the DEP Enrollment process, KACE Cloud MDM now offers full account login, including SSO for DEP authentication. This option completely eliminates the need for token authentication on iOS 13+ devices and mac 10.15+ devices .

As we continue to build out our Windows 10 support, we're introducing support for deploying Microsoft 365 for Windows. With an active Microsoft 365 subscription and KACE Cloud MDM, an admin can assign licenses to end users, set up a vendor profile, link it to a policy, and distribute Microsoft 365 to devices.

We've also made updates across all SAML-based SSO identity providers, including an improvement to automated certificate validation; new thumbprint details that include dates and status; and enhanced troubleshooting sections for each SSO identity provider.

Apple DEP Web Authentication (Mac and iOS)

Full account authentication, including SSO, is now available during the DEP enrollment process. This option eliminates the need for generating authentication tokens for iOS 13+ and mac 10.15+ devices. To enable this feature, in the DEP Profiles section, select the 'Force DEP Authentication' checkbox, then Save settings.

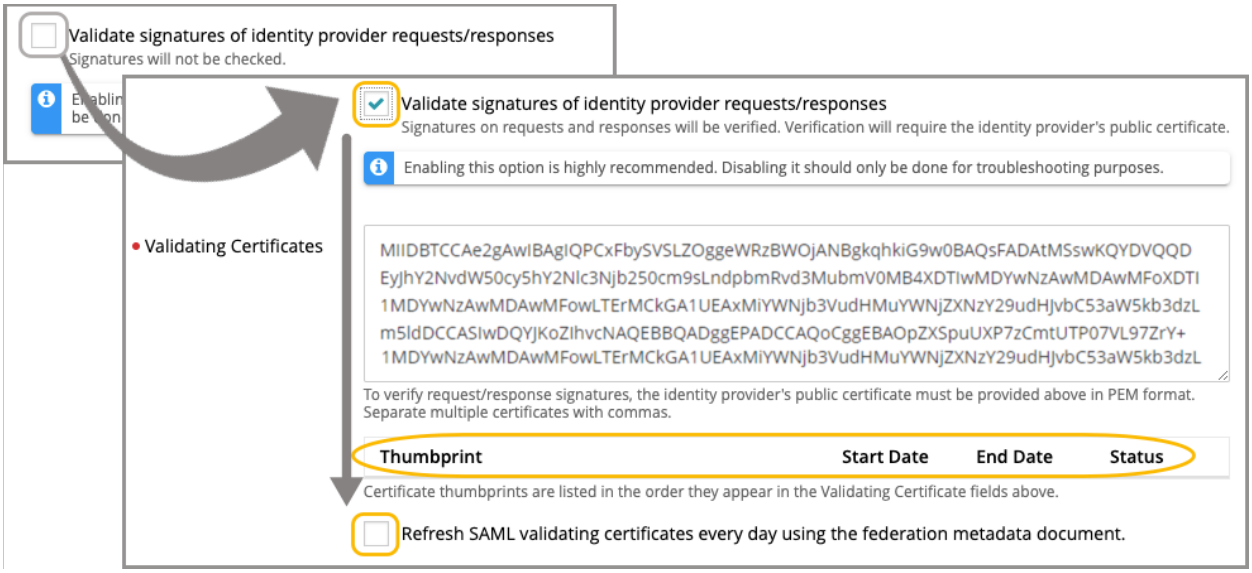


For more information on this topic, visit Apple DEP Enrollment Program in documentation.

SAML-based SSO Updates

We've made an important update to the certificate validation section on the SSO settings page. The 'Validate signatures of identity provider requests/responses' setting is now defaulted to selected, and certificates will be automatically checked and refreshed every 24 hours by KACE Cloud MDM.

The details for validated certificates will appear in the new thumbprint section, along with date and status information. To ensure daily check and refresh, an admin only needs to select the 'Refresh SAML … using Federated Metadata document' checkbox located below the thumbprint section.



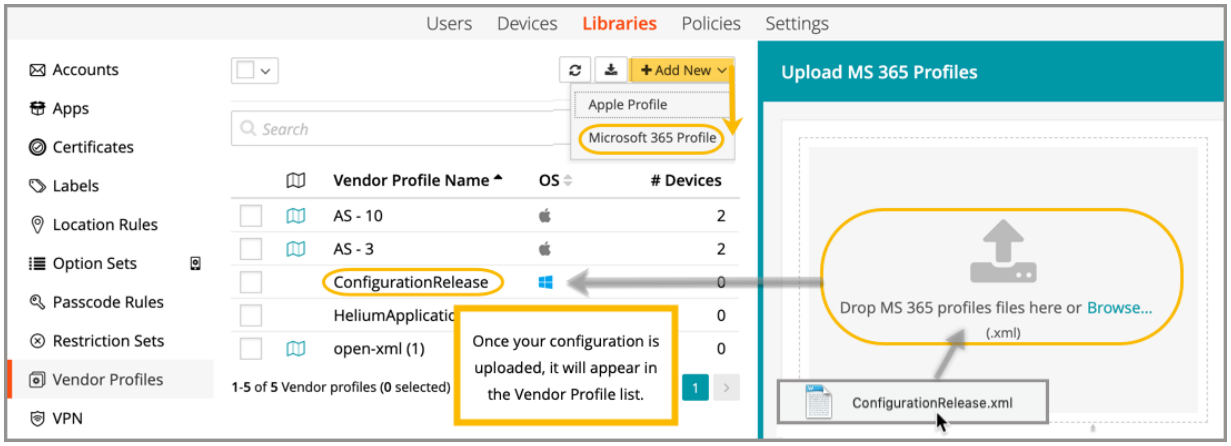
For additional information relating to this topic, please visit Single Sign-On in documentation.

Microsoft 365

Admins can now deploy Microsoft 365 to Windows devices using KACE Cloud MDM. The only pre-requisite is a Microsoft 365 subscription.

Before setting up in KACE Cloud MDM, admins should create a configuration file using the Office Customization Tool. The selections made in this file will determine what your Office 365 deployment looks like.

To set up your Microsoft 365 profile in KACE Cloud MDM, go to Libraries > Vendor Profiles > Add New > Microsoft 365 Profile, then upload and add your configuration. (Note that Apple Profiles and Microsoft 365 profiles have now been combined into a single library called Vendor Profiles.)



Once your Microsoft 365 profile is added, you can deploy it to devices using policies.

For convenience and consistency, we also recommend that you integrate Azure AD with KACE Cloud MDM. You'll find additional documentation on this topic in our Help Center: Azure AD - SSO and Windows 10 Enrollment using Azure Domain Join.

Resolved Issues

Bug fixes are included in the resolved issues list for two release periods and are then retired.

Issue	Description	Status
4518 - Unable to import the same certificate while assigning it different Windows certificate stores	Certificate can be added successfully to the same certificate to different Windows certificate stores	**FIXED**
4516 - Android 10+: Admin cannot control 'deny' or 'permanently grant' access for apps requiring background location access.	Admins can allow or disallow background location access for an app on Android 10+.	**FIXED**
4502 - Android system apps without a launcher never show as installed	App should appear as installed after inventory and device marked as compliant.	**FIXED**
4450 - Device history was showing an incorrect "Initiated by" value when a macOS Local User account was deleted or unlocked.	Correct "Initiated by" value shows when a macOS Local User account was deleted or unlocked.	**FIXED**
4425 - Android system apps deployed via policy cause device to be marked not compliant	System app shows as installed and the device as compliant.	**FIXED**
4418 - Attempting to remove a VPP app in the App Library after the MDM tenant had been disconnected from VPP in Apple Business Manager resulted in the app not being removed from the Library.	App is now removed and library updates accurately after removing a VPP app in the App Library after the MDM tenant has been disconnected from VPP in Apple Business Manager.	**FIXED**
4417 - Deploying a macOS VPP app that was missing its "short version" string would result in an exception.	When deploying a macOS VPP app that was missing its "short version" string, there are no exceptions in the log.	**FIXED**
4392 - Device history was not showing the name of the application that was updated when the associated App Configuration was updated.	Updated app name now shows in device history.	**FIXED**
macOS - macOS 10.15 Account Configuration	Resolved with release of DEP web authentication.	**FIXED**
4387 - Passcode Profile Not Recorded As Installed On macOS Device	Profile is shown as linked to the device after the command succeeds.	**FIXED**
4386 - Google play not enrolled warning message appears when trying to add iOS web app	Verified: No error message appears and create webapp form is displayed.	**FIXED**
4385 - A supervised restriction being sent to a non-supervised iPad	Verified: Restriction set installs successfully and shows up in inventory.	**FIXED**
4364 - UI: Location can be collected on demand even when the policy is turned off	Verified: Locate button is disabled or displays a message that location tracking is turned off for device. KACE Connect app does not report location when policy is set to "Off".	**FIXED**

4363 - UI: "Locate" button should not be enabled if no location policy is applied to device	Locate button disabled or displays warning that location tracking is not enabled for this device.	**FIXED**
4348 - macOS VPP Installations Not Logging Success In Device History	Verified: VPP app installed, notification shows success, device history stays submitted.	**FIXED**
4046 - Apps installed directly to a device were overwriting the information stored in the app library.	Apps installed directly to a device no longer overwrite the information stored in the app library.	**FIXED**
4031 - App list when importing to device does not show app configs	The list of apps available for adding includes one item for every App + App Config combination.	**FIXED**

Known Issues

Issue	Description	Status
4346 - Unable to Login to macOS 11.0 Device After Adding FileVault Profile	After applying a FileVault profile to a macOS 11.0 device, the device user cannot log in. This affects both virtual and physical devices.	**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**
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**

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.