BlackBerry UEM

Release Notes

12.17

Contents

BlackBerry UEM version 12.17 Release Notes

What's new in this release?

To learn about the new features introduced in every supported release of BlackBerry UEM, see What's new in BlackBerry UEM.

Installing the software

You can use the setup application to install UEM version 12.17, or to upgrade from UEM 12.15 or 12.16.x. When you upgrade the software, the setup application stops and starts all the UEM services for you. The BlackBerry UEM setup application backs up the database by default.

Note: As of UEM version 12.10, JRE is no longer bundled with the installer. If you are installing UEM, you must first download and install JRE (minimum version JRE 8u151).

Fixed issues

Fixed issues in BlackBerry UEM 12.17 MR1a quick fix 2

User, device, and app management fixed issues

On iOS devices that were enrolled in DEP, users could not remove the UEM Client from the device if it was set as the authentication delegate for BlackBerry Dynamics apps. (EMM-152603)

Fixed issues in BlackBerry UEM 12.17 MR1a quick fix 1

User, device, and app management fixed issues

Information about available updates for some iOS devices was missing when the REST API was used to get a user's device information. (EMM-151914)

The osUpdateStatus information was missing for some iOS devices if only one iOS update was available. (EMM-151439)

Fixed issues in BlackBerry UEM 12.17 MR1a

Install, upgrade and migration fixed issues

Upgrading the BlackBerry Connectivity Node from BlackBerry UEM on-premises version 12.16.1 or 12.17.0 to version 12.17.1 failed with with an Unsuccessful error message. (EMM-151666)

Fixed issues in BlackBerry UEM 12.17 MR1

Install, upgrade and migration fixed issues

If you were performing an installation in any language except English, the installation did not complete successfully when the installer couldn't find the administrator account name. (EMM-150264)

User, device, and app management fixed issues

The Device activations pop-up window accessed from the management console dashboard did not display data for activated devices. (EMM-151035)

When you enrolled a DEP device, the device might not have received the passcode enforcement policy before the passcode setup screen displayed. (EMM-151217)

When an iOS device was activated using the User privacy - User enrollment activation type, a message was displayed asking the user to upgrade to the same version of the BlackBerry UEM Client that was already installed on the device. (EMM-150754)

NullPointerException errors were written to the UEM Core log file when a user signed in to an enterprise enrolled Chrome OS device using a personal account. (EMM-150305)

For devices that you activated using the Android Enterprise - Full Control activation type, in the device's assigned IT policy, if you set the password complexity to High, and you then set the password complexity to Medium in the Work profile (all Android devices) section of the IT policy, the global setting took precedence over the Work profile setting and users were be forced to set a password with high complexity. (EMM-150252)

The BlackBerry UEM Client did not process any IT policy password complexity requirements on Android Enterprise activated Android 12 devices on BlackBerry UEM 12.16. (EMM-150137)

A security issue has been discovered that requires a BlackBerry UEM server upgrade followed by a reactivation for impacted MDM-enrolled iOS devices. For more information, visit support.blackberry.com to read article KB99869. (EMM-150054, EMM-146729)

The BlackBerry UEM Client did not retrieve or apply IT policies when the workspace was unlocked. (EMA-16864)

Android Enterprise - Full Control dualDAR activation failed when using a custom encryption app on Samsung devices running Android 10. (EMA-17112)

Policies and profiles did not get deployed on macOS 12 (Monterey) devices after they were activated. (EMM-150189)

Management console fixed issues

You could not upload an app and an app configuration using the "Upload a template" feature. (EMM-150560)

You could not remove an internal version of the BlackBerry Connectivity app in the management console. (EMM-150678)

In an org unit, if you set the "Don't Allow Users to use Parallels Desktop" option to True, when you clicked Save, an error message displayed. (EMM-150764)

In a compliance profile, the list of restricted OS versions was not listed in numerical order. (EMM-150721)

The app list did not display if the name of one of the apps in the list contained a single quote ('). (EMM-150310)

In the compliance policy, on the iOS tab, if you select the 'Show only allowed apps on device' option, add an app to the list, select the 'Restricted app is installed' option and add the same app to the Restricted apps list, when you remove the app from the Restricted apps list, it is also removed from the 'Show only allowed apps on device' list. (EMM-147897)

BlackBerry UEM Core fixed issues

The import users function might have failed when you attempted to import a large number of users. (EMM-150324)

If a user's parameters didn't match what the Google domain was expecting, the user might not have been automatically created in the Google domain. (EMM-150306)

BlackBerry Proxy fixed issues

When BlackBerry Proxy opened a connection with BlackBerry Secure Connect Plus, it took certificates from the keystore that are meant only for use with a BlackBerry Connectivity Node installation. If you did not upgrade BlackBerry UEM before the certificates expired, the UEM Client logged BlackBerry Secure Connect Plus errors that indicated failed certificate validation (EMM-150706)

Activated endpoints might have waited 15 minutes before the BlackBerry Proxy returned that they were authenticated. (EMM-148672)

Fixed issues in BlackBerry UEM 12.17 quick fix 2

Management console fixed issue

The application ID exceeded the max_int value, resulting in java.lang.NumberFormatException when trying to push an application to a device. (EMM-151300)

Fixed issues in BlackBerry UEM 12.17 quick fix 1

Management console fixed issue

An additional warning message was added to the console to assist administrators when migrating iOS devices to the hardened channel. The warning advises administrators to clear the "Remove the app from the device when the device is removed from BlackBerry UEM" option in the app settings for all applicable apps, which ensures apps are not removed during migration. (EMM-150936)

Fixed issues in BlackBerry UEM 12.17

User, device, and app management fixed issues

If you selected the "Enable USB debugging" rule in an IT policy for Android devices, the setting did not take effect until you made another change to the policy. (EMA-17249)

The BlackBerry UEM Client was logging SMS messages twice on Google Pixel devices. (EMA-17239)

Management console fixed issues

When you uploaded a .scsr file to the Apple Push Certificate Portal, an error message might have displayed. (EMM-150617)

On Chrome OS devices, device commands failed if the device was already in the state that you issued the command for. For example, if you had already disabled the device, if you issued the Disable device command again, a Command failed message displayed in the View device actions screen. (EMM-150616)

When you tried to upload an app and an app configuration using the Upload a template feature, an error displayed. (EMM-150560)

When you created a new Home screen layout profile for iOS devices and added some icons, if you then edited the layout, none of the icons displayed. (EMM-150525)

In the Parallels desktop section of an org unit, an error displayed if you made a change and clicked Save without enabling the "This field must be set to true to acknowledge the notice message associated with the field "plugin_vm_allowed" set to value "true" option. No error message displayed to indicate what caused the failure. (EMM-150499)

You could not set an app configuration to "None" in a device group. (EMM-150489)

The app configuration for an app was automatically assigned as the default when you assigned it to a device group. (EMM-150487)

When more than one Android device had a system update available, in the list of filters an incorrect string displayed instead of the text "System update available". (EMM-150438)

If you were trying to configure OpenTrust cloud PKI, after you added a trusted CA certificate in BlackBerry UEM, when you tested the connection, it failed. (EMM-150214)

On the Add apps page, some app icons did not display. (EMM-149812)

In Settings > Infrastructure > Server certificates, if you replaced one of the certificates and added a description, the description was not saved. (EMM-149599)

BlackBerry Proxy fixed issues

When you upgraded a BlackBerry Connectivity Node, the BlackBerry Proxy Service JvmMS and JvmMx values (Java Heap Variables) were overwritten, which resulted in the previous settings being lost. (EMM-149666)

Known issues

Items marked with an asterisk (*) are new for this release

Installation and migration known issues

During installation, the end user license agreement does not display in Norwegian. (EMM-150771)
After migrating a DEP device, users can remove the BlackBerry UEM profile from their device even when the "Allow removal of MDM profile" option is not selected in the DEP enrollment configuration. (EMM-150304)

User, device, and app management known issues

Note that some of these issues are for the BlackBerry UEM Client and will be fixed in a future release.

BlackBerry 10 is no longer supported. For more information, see the announcement from BlackBerry.
If a Knox Service Plugin (KSP) policy is set to disable factory reset on a device and an administrator sends an IT command to wipe the device from BlackBerry UEM, the device will be unmanaged and cannot be reactivated or complete a factory reset. (EMA-17549) **Workaround**: If devices are assigned a KSP policy that disables factory reset, create a KSP policy that allows it and assign the policy to the devices before you send the wipe command. For more information, visit https://docs.samsungknox.com/admin/knox-service-plugin/kbas to read article 844.
* After you upgrade to or install BlackBerry UEM 12.17 MR1, the log files for iOS devices are not automatically stored in the default location, C:\Program Files\BlackBerry\UEM\Logs\device_logs. (EMM-15109) **Workaround**: Specify the location to store the log files in Settings > Infrastructure > Logging > Global logging settings.
* After you set up Chrome OS device management and click on the Network tab for an org unit, an error message stating that the profile could not be retrieved might be displayed. (EMM-151438)
* An error message might be displayed when you try to save a device wallpaper image in the Device settings for a Chrome OS org unit. (EMM-151488) **Workaround**: Save the image in the Google Admin console instead.
* After you remove Apple VPP apps from a device and unassign them from the user, the license consumption counts are not updated in the UEM management console. (EMM-151299)
* When you activate a new Android Enterprise device or deactivate and reactivate an existing Android Enterprise device after upgrading to BlackBerry UEM 12.17 MR1, the device activation does not complete successfully because the CA certificate has been updated in UEM 12.17 MR1. (EMM-151249) **Workaround**: Copy and paste the new CA certificate details into the Android/Chrome management > Android Zero Touch enrollment configuration.
Chrome OS devices will not synchronize with BlackBerry UEM if they are in an org unit that has no child org units. (EMM-150375)

During the Azure AD Conditional Access enrollment flow, the user might be prompted to register the device twice. (SIS-15411)

Workaround: If the user is enrolling only in conditional access, they shouldn't open the Microsoft Authenticator app from the app store after they install it, instead they should switch to the BlackBerry UEM Client and then open the Microsoft Authenticator app.

On some devices that are configured for ZSO authentication, when the user signs in to the ZSO service through the browser, a notification prompt appears unexpectedly to choose a certificate for authentication. (EMM-147606)

Workaround: Choose the "_Cirrus_SCEP_Profile_" option.

In dark site environments, when activating a Samsung Galaxy S20 device running Android 11 with the Work and personal - full control (Android Enterprise) activation type with the premium option enabled, the device activates with the Android Enterprise workspace instead of the Knox workspace. (EMA-16736)

Users might not be prompted to set a workspace password during "Work and personal - user privacy (Android Enterprise)" activation. (EMA-16279)

If your organization uses PKI and Entrust smart credentials together, users might need to enroll the PKI certificate multiple times on the same device (maximum of once per app). (GD-35783)

Management console known issues

BlackBerry 10 is no longer supported. For more information, see the announcement from BlackBerry. Even though you will see instances of BlackBerry 10 in the console, you should no longer use those pages. All instances of BlackBerry 10 will be removed In a future release of BlackBerry UEM. (EMM-150314)

(On the Managed devices > Advanced view page, the "Available updates" filter is missing. (EMM-150933)

On the Users page, any Linked directory groups that the user is a part of do not display. (EMM-150812)

Workaround: Review the user's linked groups on the Groups page.

When you try to re-enroll a DEP-enrolled device that doesn't have the BlackBerry UEM Client installed, the following error message is displayed: "An error was encountered. The device could not be migrated." (EMM-150780)

In the Device tab of an org unit, if you schedule a device reboot and click Save, the save fails and no error message is displayed to indicate what caused the failure. Incorrect strings are also displayed in some of the fields. (EMM-150472)

You cannot synchronize Chrome OS users that have a duplicate username. (EMM-150357)

When you are configuring Azure AD Conditional Access, an error message might display and the configuration might not complete successfully due to a timeout. (SIS-15834)

Workaround: Click Ok on the error message, click Save on the Azure Active Directory Conditional Access page, and complete the configuration steps again.

When compliance override policies are applied, BlackBerry UEM might not send the compliance violation status to Microsoft Azure AD conditional access. (EMM-148486)

If you don't configure an app server for Azure AD Conditional Access in the BlackBerry Dynamics connectivity profile, Microsoft online device registration does not occur. (EMM-148453)

Workaround: In the BlackBerry Dynamics connectivity profile, add an app server for Feature-Azure Conditional Access, direct the app server to the URL of your UEM Cloud instance, and use port 443.

After a BlackBerry Dynamics app migration with one certificate, the user might display in the management console with two certificates assigned to them. (EMM-147006)

If you have added a custom image that displays in the top-left corner of the management console, when you log in to the console the default BlackBerry logo displays instead of the custom image. (EMM-146978)

The BlackBerry Connectivity app might not be delivered to an Android device that has been activated using the "Work and personal - user privacy (Samsung Knox)" activation type and "Google Play app management for Samsung Knox Workspace devices" is enabled. (EMM-136648)

Workaround: Assign the .apk file to the device as an internal app and select the 'Publish app in Google domain' option.

Component known issues

Some BlackBerry UEM components have an expired certificate bound to them. (EMM-150729)

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada