# BlackBerry UEM

## Release Notes

12.13.1

# Contents


**Installing the software..... 4**

**What's new in BlackBerry UEM 12.13 MR1.....5**

**What's new in BlackBerry UEM 12.13.....8**

**Fixed issues..... 13**

Fixed issues in BlackBerry UEM 12.13.1 quick fix 9.....13
Fixed issues in BlackBerry UEM 12.13.1 quick fix 8.....13
Fixed issues in BlackBerry UEM 12.13.1 quick fix 7.....13
Fixed issues in BlackBerry UEM 12.13.1 quick fix 6.....13
Fixed issues in BlackBerry UEM 12.13.1 quick fix 5.....14
Fixed issues in BlackBerry UEM 12.13.1 quick fix 4.....14
Fixed issues in BlackBerry UEM 12.13.1 quick fix 3.....14
Fixed issues in BlackBerry UEM 12.13.1 quick fix 2.....15
Fixed issues in BlackBerry UEM 12.13.1 quick fix 1.....15
Fixed issues in BlackBerry UEM 12.13 MR1.....16
Fixed issues in BlackBerry UEM 12.13.0 quick fix 1.....17
Fixed issues in BlackBerry UEM 12.13.....17

**Known issues in BlackBerry UEM 12.13.....19**

**Legal notice..... 22**

# Installing the software

You can use the setup application to install BlackBerry UEM version 12.13, or to upgrade from 12.11.x or 12.12.x. When you upgrade the software, the setup application stops and starts all the BlackBerry UEM services for you. The BlackBerry UEM setup application backs up the database by default.

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

# What's new in BlackBerry UEM 12.13 MR1

### Management console

- **BlackBerry 10 and the Device SR requirements profile**: BlackBerry UEM no longer supports the Device SR requirements profile for BlackBerry 10 devices. If you have a Device SR requirements profile set up for BlackBerry 10 devices, the profile settings are maintained in the UEM database, but they can't be viewed or changed in the management console.
- **Support for configuring BlackBerry Hub removed from the Email profile**: Configuring BlackBerry Hub is now supported only through app configuration. The settings for the BlackBerry Productivity Suite have been removed from the Email profile.

### BlackBerry UEM Client

- **Configuring the BlackBerry Hub app**: Administrators must now configure BlackBerry Hub through app configuration settings when supporting devices that are running UEM Client 12.37.1.156763 or later. The Email profile settings for the BlackBerry Productivity Suite are no longer supported for any version of UEM.

### BlackBerry Secure Gateway

- **BlackBerry Secure Gateway supports modern authentication**: The BlackBerry Secure Gateway now supports modern authentication to Microsoft Exchange Online (Microsoft Office 365) for iOS devices running iOS (or iPadOS) 13.0 or later and that are activated with MDM controls. You can specify the discovery endpoint and mail server resource in the BlackBerry Secure Gateway, BlackBerry Connectivity Node instances, as well as server groups. This feature is enabled in the Email profile.

### Android

- **Users are now unable to exit Android automatic enrollments**: When users set up a device enabled for Android zero-touch enrollment or Samsung Knox Mobile Enrollment for the first time or reset one of these devices to factory settings, the device automatically downloads the BlackBerry UEM Client and starts the activation process with BlackBerry UEM. If the user restarts the device before activation is complete, cancels the activation, or allows the battery to drain before activation is complete, the device automatically resets to factory settings and the activation process restarts. Users can't display the device home screen to use device features until activation is complete. This feature works for devices that are activated using the Work space only (Android Enterprise) activation type. For devices that are activated using the Work and personal - full control (Android Enterprise) activation type, a 30-minute timer was implemented that automatically resets the device to factory settings if the user is on the home screen and the device has not activated. This feature works only for Android 10 and earlier devices.
- **Support for Android 10 devices**: BlackBerry UEM profiles and functionality have been updated to support changes to the APIs that are supported by Android 10.
- **Support for activating Android devices with an NFC sticker**: Android supports using NFC stickers to initiate device activation. This functionality is similar to using the UEM Enroll app to activate devices, which is no longer supported in Android 10. You can initiate activation for an unlimited number of Android devices by tapping an NFC sticker that has been programmed with the activation details. You can view and copy the NFC client data that you need to program the sticker from the Settings > External Integration > Android Enterprise page in the management console.
- **Support for Android 11**: BlackBerry UEM now supports devices running Android 11, including support for changes to fully managed devices with a work profile in Android 11. Before upgrading devices to Android 11,

make sure that you install BlackBerry UEM Client for Android version 12.37.1.x which is required. For more information about the impact of the Android 11 upgrade, see the critical issue advisory.

### iOS

- iOS 14 and iPadOS 14 support: BlackBerry UEM now supports devices that are running iOS 14 or iPadOS 14.

### New IT policy rules

| Device type | Rule name | Description |
|---|---|---|
| iOS | Allow App Clips | Allow users to add some App Clips and remove existing App Clips on the device. |
| iOS | Allow changing diagnostic submission and app analytics settings (supervised only) | Specify whether users can change diagnostic submission and app analytics settings. |
| Android Enterprise - Global | Default SMS app | Specify the package ID of the default SMS app. On devices with Work and personal - full control activations, the app must be a pre-installed system app. |
| Android Enterprise - Global | Allow user to configure private DNS | Specify whether a user can configure private DNS, which uses TLS for DNS queries. On devices activated with Work and personal - full control, this rule is valid only on devices with Android 11 and later. |
| Android Enterprise - Global | Use opportunistic private DNS | Specify whether the DNS queries will attempt TLS and fallback when not available. |
| Android Enterprise - Global | Private DNS server | Specify the server address to use for private DNS queries. |
| Android Enterprise – Work profile | Apps allowed to access work calendar | Specify the personal app package IDs that are allowed to access the work calendar. |
| Android Enterprise – Work profile | Packages allowed to manage certificates | Specify the list of app package IDs that can manage certificate. |
| Android Enterprise – Work profile and Personal profile | Allow AI assistant to use screen content | Specify if the AI assistant on the device can use capture screen content. |
| Android Enterprise – Work profile and Personal profile | Allow AI to offer suggestions based on screen content | Specify if the AI assistant will provide selection suggestions based on screen content. |

**IT policy rule changes for Android devices with Work and personal - full control activations**

The following Android personal profile IT policy rules were deprecated for devices with Android OS 11 and later:

- Allow autofill
- Allow adding and removing accounts
- Allow installation of non Google Play apps
- Allowed system apps
- Allow printing

The following Android global IT policy rules are not supported by devices with Android OS 11 and later and the Work and personal - full control activation type:

- Allow factory reset
- Force device to use Access Point Name profile settings
- Send SMS/MMS logs to UEM
- Send SMS/MMS logs to the BlackBerry Connectivity Node
- Send phone logs to UEM
- Send phone logs to the BlackBerry Connectivity Node

The following Android global IT policy rules are no longer supported by devices with the Work and personal - full control activation type but are still supported by devices with the Work space only activation type:

- Stay awake when plugged in to AC charger
- Stay awake when plugged in to a USB charger
- Stay awake when plugged in to a wireless charger
- Allow user to configure screen timeout
- Screen timeout
- Allow user to configure screen brightness
- Force adaptive brightness
- Screen brightness
- Allow system error dialogs
- Allow ambient display
- Allow device backup

The following Android work profile IT policy rules are no longer supported by devices with the Work and personal - full control activation type but are still supported by devices with the Work space only activation type:

- Allow Android system windows

# What's new in BlackBerry UEM 12.13

### Migration

- **Migration of Android Enterprise devices**: Customers who have configured BlackBerry UEM to manage Google Play accounts can now migrate Android Enterprise devices from an on-premises BlackBerry UEM server to BlackBerry UEM Cloud or another on-premises BlackBerry UEM server. The on-premises BlackBerry UEM server must be version 12.13 or later.
- **Migration of BlackBerry Dynamics users**: You can now migrate BlackBerry Dynamics users from on-premises BlackBerry UEM (version 12.13 or later) to a BlackBerry UEM Cloud.

### Management console

- **App protection profiles update**: Microsoft Intune app protection profiles have added support for recent Microsoft Intune feature updates.
- **Specify browser**: You can now specify which browser opens web links in apps managed by Microsoft Intune.
- **Factory reset protection profile improvements**: For factory reset protection profiles, you no longer need to manually obtain the User ID when you specify Google accounts that can unlock a device that has been reset to factory settings.
- **Delete users for value-added services**: You can now delete users who have additional value-added services assigned unless the user can't be removed from the service.
- **Event notifications**: The following event notifications were added:
  - Connectivity > Service connections for UEM instance changed: This notification alerts you when the connection status changes for the BlackBerry Affinity Manager, BlackBerry Secure Gateway, BlackBerry Proxy, or BlackBerry Secure Connect Plus service.
  - Server certificates > Certificate expiry: This notification alerts you when a server certificate is about to expire.

### BlackBerry Dynamics

- **BlackBerry Dynamics screen capture detection on iOS devices**: You can enable an option in a compliance profile that reacts to screen captures of BlackBerry Dynamics apps on iOS devices. When you enable this option, you can specify the allowed number of screen captures per time period, how long a period lasts, an enforcement action to occur if the user exceeds the allowed number of screen captures, and how long the enforcement action lasts. The allowed number of screen captures is per app. If the user exceeds the number of screen captures on one app, they are prevented only from using that app, not all BlackBerry Dynamics apps.

  If you enable the option and set the enforcement action to "Monitor and log", when a user takes a screen capture, a warning message stating screen captures are prohibited is displayed on the device. If you enable the option and you set the enforcement action to "Do not allow BlackBerry Dynamics apps to run", when the user exceeds the number of screen captures, a message that informs the user how long they are prevented from taking screen captures is displayed on the device, and the user is blocked from using the app for the period that you specified in the compliance profile. All violations are logged in a compliance violation report for BlackBerry Dynamics apps.
- **Improvements to the BlackBerry Dynamics app activation process**: Administrators and users can now activate BlackBerry Dynamics apps using simple passwords (for example, a password of any length) or QR codes in addition to the 15-character access key. This simplifies the activation process for users. Activating BlackBerry Dynamics apps using a password or QR code is the preferred method of activating apps. This feature requires that apps use BlackBerry Dynamics SDK 8.0 or later.

- **Improvements to unlocking BlackBerry Dynamics apps**: Administrators can now send a QR code to a user to unlock a BlackBerry Dynamics app. Users with access to BlackBerry UEM Self-Service can use the QR code to unlock the app instead of the unlock key. This feature requires that apps use BlackBerry Dynamics SDK 8.0 or later.

#### Apple

- **Automatic activation of a BlackBerry Dynamics app for Apple DEP and User Enrollment devices**: For Apple DEP devices and devices that are activated with Apple User Enrollment, a BlackBerry Dynamics app can be preconfigured so that it automatically activates during device enrollment without requiring the user to manually enter information. If the app is an authentication delegate, it can be used to easily activate other BlackBerry Dynamics apps.
- **iOS New Capabilities**: For iOS devices with eSIM cellular plans, administrators can request updated plan information from the carrier.

#### Chrome OS

- **Management of Chrome OS devices**: You can now manage Chrome OS devices separately from Android devices in the following ways:
  - On the Dashboard, in Devices by platform, Chrome OS devices are shown.
  - In Users > Managed devices, Chrome is now an option for the OS filter.
  - In Groups > Device, you can create device groups based on Chrome OS.
  - In Migration > Migrate devices, Chrome OS devices are shown

#### IPv6

- **IPv6**: BlackBerry UEM components now support IPv6, with the exception of components related to BlackBerry 10. Note that BlackBerry 10 devices have not been tested in an IPv6 environments.

#### Windows 10 devices

- **Support for Windows Hello for Business**: For Windows 10 devices, you can now choose whether to allow biometric gestures (such as facial or fingerprint recognition) in the IT policy. You can also enable enhanced anti-spoofing for when facial recognition is configured on the device. These settings require Windows 10 version 1511 or later.

#### Documentation

- The BlackBerry Docs site has improved search and navigation tools to make it easier to find docs for products and features. Click the magnifying glass in the top navigation bar to perform a keyword search. You can filter results by product, version, and document type.

  You can also click **Let us help you find something** on the home page and BlackBerry UEM page to open a Doc Map that will point you to the right doc, whether you're looking for product information to help make a purchase decision or you're already a customer and need administrator, end-user, or developer help.
- A beta version of an easy-to-use online version of the Performance Calculator will be available soon. You will be able to access it on the BlackBerry UEM Planning and architecture documentation web page.

**New IT policy rules**

| Device type | Name | Description | Activation types |
|---|---|---|---|
| Windows | Allow use of biometric gestures | Enable or disable the use of biometric gestures, such as face and fingerprint, as an alternative to the PIN gesture for Windows Hello for Business. | MDM controls |
| Windows | Enable enhanced anti-spoofing for facial feature recognition | Enable or disable enhanced anti-spoofing for facial feature recognition on Windows Hello face authentication. | MDM controls |
| Android Global (all Android devices) | Obtain time zone from network | Specify whether the device obtains the time zone from the network. | Work space only, Work and personal - full control |
| Android Global (all Android devices) | Device time zone | Specify the time zone that the device uses. For a list of possible values, see the IT Policy Reference. | Work space only, Work and personal - full control |
| Android Global (all Android devices) | Allow ambient display | Specify whether the user can enable ambient display on the device. Ambient display shows notifications on the lock screen when the device is locked. | Work space only, Work and personal - full control |
| Android Global (all Android devices) | Allow airplane mode | Specify whether the user can enable airplane mode on the device. | Work space only, Work and personal - full control |
| Android Work profile (all Android devices) | Force the device and work profile passwords to be different | Specify whether the device and work profile passwords must be different when a work profile password is required by the Android work profiles "Password requirements" rule. | Work and personal - user privacy, Work and personal - full control |

| Device type | Name | Description | Activation types |
|---|---|---|---|
| Android Work profile (all Android devices) | Allow printing | Specify whether the user can print files using the device OS print functionality. This rule does not block sharing files to apps that can send files to a printer. | Work space only, Work and personal - user privacy, Work and personal - full control |
| Android Work profile (all Android devices) | Allow user to configure location | Specify whether the user can turn the location feature on or off. | Work space only, Work and personal - user privacy, Work and personal - full control |
| Android Work profile (all Android devices) | Allow personal data in work profile | Specify whether files and data in the personal profile can be sent to the work profile or accessed from work apps. | Work and personal - user privacy, Work and personal - full control |
| Android Work profile (all Android devices) | Allow biometrics | Specify whether the user can use biometric authentication to unlock the device. | Work space only, Work and personal - user privacy, Work and personal - full control |
| Android Work profile (all Android devices) | Allow facial recognition | Specify whether the user can unlock the device using face recognition. | Work space only, Work and personal - user privacy, Work and personal - full control |
| Android Work profile (all Android devices) | Allow iris authentication | Specify whether the user can unlock the device using an iris scan. | Work space only, Work and personal - user privacy, Work and personal - full control |
| Android Work profile (all Android devices) | Apps restricted from metered networks | Specify the apps that are restricted from using metered data networks. You may want to restrict app network usage due to data costs and limits or battery and performance issues. | Work space only, Work and personal - user privacy, Work and personal - full control |
| Android Personal profile (all Android devices) | Allow biometrics | Specify whether the user can use biometric authentication to unlock the device. | Work and personal - full control |

| Device type | Name | Description | Activation types |
|---|---|---|---|
| Android Personal profile (all Android devices) | Allow facial recognition | Specify whether the user can unlock the device using face recognition. | Work and personal - full control |
| Android Personal profile (all Android devices) | Allow iris authentication | Specify whether the user can unlock the device using an iris scan. | Work and personal - full control |
| Android Personal profile (all Android devices) | Allow printing | Specify whether the user can print files using the device OS print functionality. This rule does not block sharing files to apps that can send files to a printer. | Work and personal - full control |

# Fixed issues

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 9

**Device fixed issue**

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)

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 8

**User and device fixed issue**

Setting any IT policy password option caused iOS 15 and iPadOS 15 devices to reject the policy. (EMM-148414)

**JRE fixed issue**

UEM was not compatible with JRE 8u301. (EMM-148416)

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 7

**Database fixed issues**

On upgrade, the hardware model name didn't update due to a duplicate entry in the database. (EMM-145735)

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 6

**JRE fixed issues**

If you had installed JRE version 8u291 or 8u292, you could not install new instances of BlackBerry UEM. (EMM-147601)

**Migration fixed issues**

Good Control to BlackBerry UEM migration did not complete when there was duplicate data being migrated from the source Good Control database. (EMM-147471)

#### Database fixed issues

| |
|---|
| Database transactions did not complete when the scheduler queue grew too large because there was no timeout value set. (EMM-147270) |

#### API fixed issues

| |
|---|
| The REST API call used to update the device OS model returned a 400 error. (EMM-147435) |

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 5

#### Migration fixed issue

| |
|---|
| The Migration controller timeout was increased for when you're migrating devices from Good Control to BlackBerry UEM. (EMM-147225) |

#### BlackBerry Dynamics app fixed issue

| |
|---|
| Some BlackBerry Dynamics apps could be sideloaded on iOS devices. (EMM-147014) |

#### BlackBerry Proxy fixed issue

| |
|---|
| The BlackBerry Proxy buffer size was increased when there is a TCP Window scale factor configured. (EMM-147382) |

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 4

#### BlackBerry Secure Connect Plus fixed issue

| |
|---|
| BlackBerry Secure Connect Plus might have stopped working intermittently causing users to lose connection. (EMM-146811) |

## Fixed issues in BlackBerry UEM 12.13.1 quick fix 3

#### Management console fixed issues

| |
|---|
| If the BlackBerry Core returned a 404 error in response to a call from the management console, the console did not detect the error for approximately 30 seconds. (EMM-145826) |

| |
|---|
| If an iOS device was part of a device group that was based on OS version, after you upgraded the OS on the device it wasn't automatically assigned to a new device group. For example, if your organization has device groups for iOS 13.5 and iOS 13.5.1, when you upgraded an iOS 13.5 device to 13.5.1, it was not automatically assigned to the new group. (EMM-145130) |

**App fixed issues**

| |
|---|
| After upgrading to BlackBerry Connectivity version 1.22.0.884, all other BlackBerry apps stopped working. (EMM-146828) |
| When the Samsung KSP app was updated to the latest version, all of the fields in the associated app config were reset. (EMM-146342) |

**BlackBerry UEM Core fixed issues**

| |
|---|
| BlackBerry UEM Core can now handle multiple simultaneous app updates so that all updates will complete successfully. (EMM-146604) |

# Fixed issues in BlackBerry UEM 12.13.1 quick fix 2

**Management console fixed issues**

| |
|---|
| An error displayed in the log files when an entry in the user row did not match the entry in the user ID column in the UEM database because the user had been removed. (EMM-146002) |

**User and device management fixed issues**

| |
|---|
| Users could not activate iOS devices if a SQL Select query timed out when fetching policies. (EMM-146496) |
| Users could enroll Android devices when the PKI certificates did not match. (EMM-142876) |

# Fixed issues in BlackBerry UEM 12.13.1 quick fix 1

**Management console fixed issues**

| |
|---|
| When you created an Enterprise Connectivity profile for Android devices, you might not have been able to add many apps to the 'Apps restricted from using BlackBerry Secure Connect Plus" section because of a database field size restriction. (EMM-145722) |

#### User and device management fixed issues

| |
|---|
| DEP enrolled devices did not get per-app VPN configuration and app policy information when apps were first pushed to the devices. (EMM-145963) |

#### REST API fixed issues

| |
|---|
| If multiple BlackBerry Connectivity Nodes were turned off, an HTTP 500 error occurred when using the Get servers REST API call (/api/v1/servers). (EMM-145800) |

## Fixed issues in BlackBerry UEM 12.13 MR1

#### Installation and migration fixed issues

| |
|---|
| After an upgrade to BlackBerry UEM 12.12.1, you might not have been able to log into the management console using certificate-based authentication due to a port number change. (EMM-143848) |

#### User and device management fixed issues

| |
|---|
| DNS calls to internal servers might have timed out if your environment blocked DNS calls with the ANY filter. (EMM-144777) |
| On an Android Enterprise device, users could turn the location feature on even if the setting was turned off by the IT policy. (EMM-143162) |
| The BlackBerry UEM Core did not send the Device IMEI value to the Lookout for Work app when the app activated. (EMM-140895) |
| If a junior help desk administrator did not have the "View factory reset protection profiles" permission enabled, an error occurred when the junior help desk administrator clicked on a user. (EID-12919) |

#### Management console fixed issues

| |
|---|
| If you installed the console on its own server, you could not create or edit BlackBerry Dynamics Connectivity profiles while logged into the standalone console. (EMM-144498) |
| When you clicked "Add" in the "App servers" section of a BlackBerry Dynamics connectivity profile, any apps that had multiple binaries were duplicated on the 'Select a BlackBerry Dynamics app' page. (EMM-143152) |
| If you used custom self-service activation messages and the custom message contained %ActivationQRCode % as part of the message, users couldn't set their own activation passwords in BlackBerry UEM Self-Service. (EMM-142869) |

# Fixed issues in BlackBerry UEM 12.13.0 quick fix 1

**Management console fixed issues**

| |
|---|
| For any BlackBerry Dynamics apps that were assigned in an app group, on the device details page the status of the apps displayed as 'Not activated', and app actions such as lock and debug logging were not available. (EMM-144742) |
| You couldn't save a DEP enrollment configuration if you set the "Allow removal of MDM Profile" option to Off. (EMM-144491) |

# Fixed issues in BlackBerry UEM 12.13

**Management console fixed issues**

| |
|---|
| After you upgraded BlackBerry UEM, a user with the Junior HelpDesk role could not set an activation password. (EMM-142625) |
| When you tried to use the "Change password and lock device" command in the management console for a device that was activated using an Android Enterprise activation type, if you had configured the IT policy to use 'Numeric Complex' passwords, an error displayed that stated the password did not meet the minimum requirements. (EMM-141537) |
| App configurations for BlackBerry Dynamics apps did not display in the console if the name of the app configuration contained an apostrophe. (EMM-141440) |
| You might not have been able to remove a VPP account that had many users. (EMM-141084) |
| If an administrator did not have the "View User Credential Profile" permission assigned and you created a user credential profile to manually upload certificates, the administrator could not upload or replace certificates. (EMM-141001) |
| After you created a VPN profile for Juniper Pulse Secure, when the profile was sent to the device, some of the fields were missing. (EMM-140846) |
| The "Tenant attestation enabled date" was updated in the database when you clicked Save on the Attestation page. (EMM-140416) |
| In an IT policy for Android devices, the tooltip for the "Apps allowed to access external storage" option stated that the option could be applied to devices activated using the "Work space only (Premium)" activation type but it could not. (EMM-138293) |
| On the device tab, if you tried to upgrade the software version on a supervised iOS device to a specific version number, when you clicked on Download and install, the OS was downloaded but not installed. (EMM-135440) |

### BlackBerry Secure Connect Plus fixed issues

| |
|---|
| After you upgraded to BlackBerry UEM 12.12, the BlackBerry Secure Connect Plus service might not have started and stayed running if syslog was configured for localhost. (EMM-139980) |

# Known issues in BlackBerry UEM 12.13

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

#### APNs and BlackBerry Connectivity Node Known issues

If you have installed JRE version 8u291 or 8u292, you might see the following issues: (EMM-147596)

- Unable to test or renew the APNs certificate
- Unable to activate a BlackBerry Connectivity Node

#### Installation and migration known issues

During migration, after you refresh the "Migrate users" page, sometimes no records are displayed. (EMM-143257)

After migration is complete, a user group might not have a migrated BlackBerry Dynamics profile associated with it if the user group is associated with a BlackBerry Dynamics profile and a BlackBerry Dynamics connectivity profile. (EMM-142794)

If you deploy Microsoft SQL Server Express 2017 SP1 to use with BlackBerry UEM, the database setting AutoClose might be set to true instead of false. (EMM-142788)

**Workaround**: In the Microsoft SQL Server Management Studio, right click on the BlackBerry UEM database and set AutoClose to false.

When you migrate an app, some of the app configuration settings might be lost. (EMM-142673)

**Workaround**: Set the app configuration values manually.

#### User and device management known issues

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

* If you are using the BlackBerry UEM Client as the primary authentication delegate for BlackBerry Dynamics apps on supervised iOS devices, users can uninstall and reinstall the BlackBerry UEM Client, which forces them to reset the BlackBerry Dynamics password. (EMM-145824)

**Workarounds**:

For supervised iOS devices, do not set the BlackBerry UEM Client as the primary authentication delegate. Instead use one of the BlackBerry Dynamics productivity apps such as BlackBerry Work or BlackBerry Notes as the authentication delegate.

Or

For BlackBerry UEM 12.13.1 or later, you can restrict supervised iOS devices that are running iOS 14 or later from uninstalling UEM Client and other managed apps. In the management console navigate to Apps > BlackBerry UEM Client > Settings > iOS tab > and deselect the Removable App option.

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)

The 'Do not allow Android dictation' option in the BlackBerry Dynamics profile is used to stop dictation from keyboards, however there are certain keyboards that allow dictation through other channels. (GD-35440)

**Workaround**: To help mitigate the issue, you can apply an IT policy with the 'Allowed input methods' option set to 'System only' or enforce installation of particular keyboards in the Android work profile.

After an iOS user imports a certificate, the user is taken through the import process again. (G3IOS-18108)

#### Management console known issues

* If you navigate to Settings > BlackBerry Protect > Safe browsing, and you click the online help icon (?), you are directed to the incorrect page. The correct page is Safe browsing with BlackBerry Dynamics apps. (EMM-145713)

* If you create an app configuration that contains a slash (\), after you save the app configuration and exit the app settings screen, when you open the app settings again, no app configurations display. (EMM-145626)

**Workaround**: Do not create an app config that contains a slash.

* If an administrator uses a custom role and is permitted to manage only selected groups, they might not be able to enable the 'Turn on lost mode' setting for devices. (EMM-145473)

**Workaround**: Allow the custom administrator role to manage all groups.

* If you use Google Chrome to view the console, and are setting up a connection with Microsoft Intune, when you select the 'Modern Authentication' option and enter the user name and password, the console might stop responding. Also, if you select the 'Modern Authentication' option and then switch to 'Client credentials authentication', and then back to 'Modern authentication', the console might stop responding. (EMM-145542)

**Workaround**: Refresh the console or close and reopen the browser.

* You can edit the name of an Device SR profile but when you click Save, an error displays. Also, if you are using the console in Spanish, you cannot edit or create a new Device SR profile. (EMM-144919)

If you use a REST call to create a compliance policy and you set the iOS hardware restriction to false, the error message that displays does not provide the administrator with enough information to successfully create the profile. (EMM-140868)

A message does not display in the console when a BlackBerry Dynamics connectivity verification compliance violation occurs. (EMM-137201)

A per-app VPN connection cannot be established on a device that is activated with the 'User privacy – User enrollment' activation type. (EMM-136964)

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.

| |
|---|
| When you add an internal app and an icon for the app, if you click the Refresh button on the Apps page, the icon does not display in the list of apps. (EMM-134638) |
| Apps do not get unblocked after adding a corresponding version to *my*Account and synchronizing the app with BlackBerry UEM. (GD-45067) |
| When you are using the Advanced view in the management console, the device details page displays the incorrect Total internal storage amount for devices. (EMM-98304) |
| You can't update the version of an app in the BlackBerry UEM console before the newer version of the app is available in Google Play. (EMM-89974)<br>**Workaround**: Add the new version of the app to Google Play, wait for Google to publish the app and then add the app to the BlackBerry UEM console |

# 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 .https://www.blackberry.com/us/en/legal/third-party-software

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