



# BlackBerry UEM

## Release notes

12.10



# Contents

- Installing or upgrading the software..... 4**
- What's new in BlackBerry UEM 12.10.....5**
- Fixed issues..... 13**
- Known issues in BlackBerry UEM 12.10..... 14**
- Maintenance releases of the BlackBerry Connectivity app.....20**
- Legal notice..... 21**

# Installing or upgrading the software

You can use the setup application to install BlackBerry UEM version 12.10 or to upgrade from BlackBerry UEM version 12.9.x or BlackBerry UEM version 12.8.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.

# What's new in BlackBerry UEM 12.10

## Android

**Enable Android Enterprise for all Android Enterprise instances:** The configuration wizard that appears on initial log in to BlackBerry UEM now allows administrators to configure Android Enterprise. (JI 2539585)

Android SafetyNet improvements: The following improvements were made for Android SafetyNet support:

- A Google SafetyNet attestation failure option was added to the compliance profile. This option creates a compliance rule that specifies the actions that occur if devices do not pass SafetyNet attestation.
- An app grace period was added to the Android SafetyNet configuration.
- You can add a list of BlackBerry Dynamics apps that receive attestation challenges.

**Policies for Android Enterprise devices:** Policies have been added for logging of SMS, MMS and phone calls on Android Enterprise devices. You can enable the logging in a server group or in the default settings of the BlackBerry Connectivity Node setup page. You must upgrade the BlackBerry Connectivity Node to the most recent version before you can use this feature. (JI 856189)

**Specify which certificates are used with Android apps:** A new certificate mapping profile allows you to specify which user credential, SCEP, or shared certificate profile is used when an Android app requires a certificate. (JI 2517869)

**Android app-based PKI:** You can now use an app-based PKI solution such as Purebred with BlackBerry Dynamics apps on Android devices. (JI 1965015)

**Samsung KNOX support:** BlackBerry UEM now supports devices running Samsung KNOX 3.2. (JI 2573555)

**Support for Samsung KNOX policies on Android Enterprise for all BlackBerry UEM activations:** The benefits of Samsung KNOX are now available to Samsung KNOX devices when the devices are activated with an Android Enterprise activation type. Samsung KNOX devices that are activated with an Android Enterprise activation type now have Samsung KNOX policies applied. Even though devices already activated with a Samsung KNOX activation type continue to work, the Android Enterprise activation types are recommended for new activations. (JI 2510232)

Samsung KNOX activation type	Recommended Android Enterprise activation type
Work and personal - full control (Samsung KNOX)	Not applicable. Continue to use the Work and personal - full control (Samsung KNOX) activation type.
Work and personal - user privacy - (Samsung KNOX)	Work and personal - user privacy - (Android Enterprise): No KNOX policies are applied to the device. If you want to apply KNOX policies in the work space, select "When activating Android Enterprise) devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus"

Work space only - (Samsung KNOX)

Work space only (Android Enterprise): KNOX MDM policies are applied to the device. If you want to apply KNOX policies in the work space, select "When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus."

## iOS

**Event notification:** A new Administration section was added to the Event notifications page. The section contains a field that allows you to set up a notification that is sent when an administrator account gets locked. (JI 2529062)

**Device unenrollment notification:** The event notification that you receive for device unenrollment now includes the reason that the unenrollment occurred. (JI 2565941)

**New S/MIME settings:** New settings are available for iOS 12 and later devices. (JI 2571842)

iOS: email profile settings	Description
User can toggle S/MIME signing	This setting specifies whether a user is allowed to turn the signing setting on/off. This setting applies only to iOS 12.0 and later devices
User can change signing credentials	This setting specifies whether a user is allowed to change signing credentials. This setting applies only to iOS 12.0 and later devices.
User can override S/MIME encryption	This setting specifies whether a user is allowed to turn the encryption setting on/off. This setting applies only to iOS 12.0 and later devices.
User can override S/MIME encryption credentials	This setting specifies whether a user is allowed to change S/MIME encryption credentials. This setting applies only to iOS 12.0 and later devices.

**Per-app notification:** When you are configuring per-app notifications for an iOS device, you can select the following new options:

- **Enable critical alert:** This option specifies whether a critical alert can override the do not disturb profile and notification settings. This setting applies only to iOS 12.0 and later devices.
- **Show in CarPlay:** This option specifies whether notifications display in Apple CarPlay. This setting applies only to iOS 12.0 and later devices.

**Work app catalog search:** Users can now perform a search in the work app catalog to easily find apps that are assigned to them.

## BlackBerry Dynamics

**App deployment reports:** For BlackBerry Dynamics apps, you can export app deployment reports to an .html file from the Apps screen in the management console. The report includes information about apps deployed by BlackBerry UEM and the users that have installed the apps on their devices. The report now includes a Status column that provides a status of the apps on each device, such as installed and not installed. (JI 2565954)

**BlackBerry Dynamics access key email:** When you generate BlackBerry Dynamics access keys for a user, you can specify whether to send an activation email to the user. (JI 2578997)

**SCEP improvement:** You can now configure BlackBerry Dynamics apps to use SCEP to retrieve certificates. (JI 2532872)

**Installation**

**Remove BlackBerry Collaboration Service, JRE, and JCE deployment from setup.exe:** As of BlackBerry UEM release 12.10, the BlackBerry Collaboration Service and JRE are no longer bundled with the installer. If you are installing BlackBerry UEM, you must first download and install JRE (minimum version JRE 8u151).

**Certificates**

Certificate-based authentication improvement: BlackBerry UEM now supports certificate-based authentication for logging in to the management console and UEM Self-Service. (JI 1465040)

**BlackBerry UEM Notifications**

**User synchronization service from UEM:** UEM administrators can now ensure all of their users are in the BlackBerry AtHoc system by synchronizing users from within the UEM console. Administrators can set up a user synchronization service as a system job that updates users periodically and keeps track of the changes.

**New IT policy rules**

Device type	Group	Name	Description
Android	Global (all Android devices)	Allow outgoing calls	Specify if a user can place outgoing calls. If this rule is not selected, the device can only make emergency calls. All other outgoing calls are blocked.
Android	Global (all Android devices)	Send SMS/MMS logs to the BlackBerry Connectivity Node	Specify whether the device synchronizes logs for SMS text messages and MMS messages with your EMM server.
Android	Global (all Android devices)	Send phone logs to the BlackBerry Connectivity Node	Specify whether the device synchronizes the call log for the Phone app with your EMM server.
Android	Global (Samsung KNOX devices only)	Allow NFC	Specify whether a device can use NFC.
Android	Global (Samsung KNOX devices only)	Allow OTA updates	Specify if a device can update its OS using a Firmware Over-The-Air (FOTA) client (for example, Samsung KNOX EMM or WebSync DM). If this rule is not selected, all wireless update requests (user-initiated, server-initiated, and system-initiated) are blocked. The user may see messages related to new OS updates but any attempt to update the OS fails.

Device type	Group	Name	Description
Android	Global (Samsung KNOX devices only)	Allow Wi-Fi	Specify whether a device can make Wi-Fi connections. After you deselect this rule and then reselect it, the device cannot use Wi-Fi until it is restarted.
Android	Global (Samsung KNOX devices only)	Allow Wi-Fi Direct	Specify if a device can use Wi-Fi Direct. When this rule is selected, the device can make connections using Wi-Fi Direct. This rule also affects the S Beam feature on Samsung devices.
Android	Global (Samsung KNOX devices only)	Allow tethering	Specify if a device can share its mobile network connection with other devices using Bluetooth. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow Bluetooth tethering	Specify if a device can share its mobile network connection with other devices using Bluetooth. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow USB tethering	Specify if a device can share its mobile network connection with other devices using USB. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow Wi-Fi tethering	Specify if a device can share its mobile network connection with other devices using Wi-Fi. If this rule is not selected, the user cannot change this setting on the device.
Android	Global (Samsung KNOX devices only)	Allow firmware recovery	Specify if a user can update the operating system of a device using download mode.
Android	Global (Samsung KNOX devices only)	Require SD card encryption	Specify if a device must encrypt all data on the external SD card. This rule requires the value of the "Password requirements" rule to be at least "Alphanumeric."



Device type	Group	Name	Description
Android	Work profile (Samsung KNOX devices only)	Require certificate revocation (CRL) check for apps	Specify if apps must check for revoked certificates in the server certificate chain when opening SSL connections in KNOX Workspace . This rule applies only to apps that use the standard Java SSL sockets and TrustManager implementation (including most native apps), but does not apply to third-party browsers. The certificate revocation check uses CRLs from the CRL distribution point listed in the certificates. If the "Require OCSP check" rule is selected, apps first check for certificate revocation using OCSP. If OCSP fails, then apps check the CRLs.
Android	Work profile (Samsung KNOX devices only)	Require OCSP check for apps	Specify if apps must use OCSP before using CRLs to check for revoked certificates when opening SSL connections in KNOX Workspace. The OCSP check uses the OCSP response server in the "Authority Information Access" extension in the certificate.
Android	Work profile (Samsung KNOX devices only)	Validate end-user installed certificates	Specify whether the device validates certificates installed by end users. If one of the validation checks (for example, certification path, expiration date, or revocation status) fails, the device blocks the installation of the certificate.
Android	Work profile (Samsung KNOX devices only)	Allow "Share via" list	Specify whether a work app can display the "Share via" list to allow a user to share content across work apps in the Workspace.
Android	Work profile (Samsung KNOX devices only)	Allow audio recording	Specify whether a device can record audio. If this rule is not selected, the user can still make calls and use audio streaming using the device microphone. This rule applies to phone calls, voice recognition, and VoIP. If an app declares a use type and does something else, then this rule cannot block the app. If you deselect this rule, any ongoing audio recording is interrupted. Video recording is still allowed if no audio recording is attempted. This rule applies to the Workspace only.

Device type	Group	Name	Description
Android	Work profile (Samsung KNOX devices only)	Allow Google auto-sync	Specify if Google accounts and apps can sync automatically. This rule does not block Google Play from updating installed apps. Users can still manually sync from some apps, including Gmail.
Android	Work profile (Samsung KNOX devices only)	Allow video recording	Specify if a device can record video. If this rule is not selected, the camera is still available so that a user can take pictures and use video streaming. If you deselect this rule, any ongoing video recording is interrupted.
Android	Work profile (Samsung KNOX devices only)	Enable JavaScript	Specify whether the native Android browser prevents the browser from running JavaScript code for a website. If this rule is not selected, a website that requires JavaScript to be active to execute a function (for example, an animation) cannot execute the function. If this rule is not selected, a user cannot change the setting on the device.
Android	Work profile (Samsung KNOX devices only)	Allow fingerprint authentication	Specify whether the user can use fingerprint authentication for the KNOX Workspace.
Android	Work profile (Samsung KNOX devices only)	Allow iris authentication	Specify whether a user can authenticate with the work space using an iris scan.
Android	Work profile (Samsung KNOX devices only)	Allow password visibility	Specify whether the Workspace password is visible when a user is typing it. If this rule is not selected, users and apps cannot change the visibility setting.
iOS	Security and privacy	Allow managed apps to add contacts to unmanaged accounts	Specify whether users can add contacts from managed apps to unmanaged contacts accounts.
iOS	Security and privacy	Allow unmanaged apps to read contacts from managed accounts (supervised only)	Specify whether unmanaged apps can read contacts from managed contacts accounts.

Device type	Group	Name	Description
Windows Phone	Security and privacy	Default app access to diagnostic information	Specify whether apps can access device diagnostic information about other apps by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access diagnostic information. If you select "Disallow," apps can't access diagnostic information.
Windows Phone	Security and privacy	Apps allowed access to diagnostic information	Specify the list of apps that are always allowed to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule.
Windows Phone	Security and privacy	Apps not allowed access to diagnostic information	Specify the list of apps that are never allowed to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule.
Windows Phone	Security and privacy	App access to diagnostic information controlled by user	Specify the list of apps that users can choose to allow to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule.
Windows Phone	Security and privacy	Default apps can run in background	Specify whether apps can run in background by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can run in background. If you select "Disallow," apps can't run in background.
Windows Phone	Security and privacy	Apps allowed to run in background	Specify the list of apps that are always allowed to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule.

Device type	Group	Name	Description
Windows Phone	Security and privacy	Apps not allowed to run in background	Specify the list of apps that are never allowed to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule.
Windows Phone	Security and privacy	App ability to run in background controlled by user	Specify the list of apps that users can choose to allow to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule.

# Fixed issues

## Installation, upgrade, and migration fixed issues

After you upgraded to BlackBerry UEM 12.9 MR1, some BlackBerry Enterprise Identity tenant synchronizations might not have completed. (JI 2612647)

When you upgraded from BlackBerry UEM 12.9 to BlackBerry UEM 12.9 MR1, if the file path contained brackets (), the upgrade might have failed. For example, this file path did not allow the upgrade to complete: C:\users\besadmin\downloads\upgrade(x.xx.xx). (JI 2611366)

When you installed a BlackBerry Router you could not change any of the SRP settings, such as SRP host. (JI 2572218)

When you were migrating devices from Good Control to BlackBerry UEM, if you refreshed the cache on the migrate device page and the user had an associated device, and then in Good Control you added another device for the same user, migrated the user and the user's new device, and did not refresh the cache, the new device did not display on the Device migration status page. (JI 2519995)

## User and device management fixed issues

You could not use KNOX Mobile Enrollment if you were using BlackBerry UEM in a dark site environment. (JI 2578834)

## Management console fixed issues

If you created a user certificate that had only LDAP CRL URIs specified, if the certificate was revoked, the user could still log in to the BlackBerry UEM management console. (JI 2637962)

In a user credential profile, you could change the certificate type after you assigned the profile to a device. (JI 2580374)

If you navigated to Settings > Infrastructure > Logging > Global logging settings and changed the Maximum server log file age, the BlackBerry Proxy log files that were older than the number of days that you entered were not removed. (JI 2577785)

# Known issues in BlackBerry UEM 12.10

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

## Deprecation of the MDM Controls activation type

Google is deprecating the MDM Controls activation type in an upcoming release of the Android operating system. For more information, visit [support.blackberry.com/kb](https://support.blackberry.com/kb) to read KB48386.

## Installation, upgrade, and migration known issues

\* After upgrading, in the management console, BlackBerry Proxy is not visible in the cluster. For more information visit [support.blackberry.com](https://support.blackberry.com) to read [KB53554](#). (JI 2654528)

**Workaround:** Upgrade your organization's BlackBerry Connectivity Node to version 2.4

\* The installer might not restart services after an upgrade is complete. (JI 2638109)

**Workaround:** Manually start the services.

\* The BlackBerry Router installation log files are not moved to the deployment folder after installation is complete. (JI 2634654)

**Workaround:** You can find the log files in the temp folder.

\* You cannot install a BlackBerry Router if you specify a service account name and password in the `deployer.properties` file. (JI 2634648)

**Workaround:** Leave the username and password fields empty.

Some app configurations might not migrate from Good Control to BlackBerry UEM. (JI 2521111)

When you are migrating apps from Good Control to BlackBerry UEM, if you have not configured a policy that contains an authentication delegate in Good Control but BlackBerry UEM has a policy that configures app A as an authentication delegate, when you migrate app B, the app is blocked from migrating because app A has not been migrated. If you then migrate app A, app B will still be blocked because it does not send a request to app A to see if it has been migrated. (JI 2507114)

**Workaround:** On the device, force the apps to stop and then restart app B.

## 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.

\* On iOS devices, the BlackBerry UEM Client might remain in a non-compliant state even after the user removes the restricted app. (JI 2652700)

**Workaround:** Reactivate the BlackBerry UEM Client.

\* When a device user taps on a notification that an app has been assigned, the app does not display on the New tab. (JI 2642976)

**Workaround:** Tap on the All tab or the Required tab, and then tap on the New tab and install the app.

\* You might not be able to activate a BlackBerry Dynamics app that is deployed as a privately targeted app in Google Play. (JI 2642724)

\* After you create an app shortcut for an iOS device user, the user cannot open the shortcut on the device. (JI 2642617)

\* If a user switches devices, the UEM Client might be blocked. (JI 2642027)

\* If you upload an apk file that has an ampersand (&) in the title, after you assigned the app to a user, you can not activate the user. (JI 2640510)

\* Gatekeeping might not work for BlackBerry Hub+ users. (JI 2638156)

\* When a user activates an iOS device and sets their own activation password, they might receive an unnecessary email about activating BlackBerry Dynamics apps. (JI 2635013)

On an Android 9 device, if the Prevent Screen Capture security policy setting is disabled, the user can cut/copy/share data from a BlackBerry Dynamics app to a non-BlackBerry Dynamics app, even when data leakage prevention (DLP) is enabled via Pixel Launcher functionality. To ensure no data leakage, it is recommended that you enable the Prevent Screen Capture policy setting. (JI 2598556)

You can't use the Purebred app and Entrust smart credentials at the same time on iOS devices with BlackBerry Dynamics. If you do, the Purebred certificate is imported on the incorrect user credential profile. (JI 2585322)

If your organization is using Entrust smart credentials, BlackBerry Work might stop responding after a user taps Next when the Certificate Required message displays. (JI 2581797)

**Workaround:** Restart BlackBerry Work.

\* For BlackBerry 2FA to work on Android devices, you must upgrade the UEM Client to version 12.390.155029. (JI 2581256)

\* For BlackBerry 2FA to work on iOS devices, you must upgrade the UEM Client to version 12.38.2127. (JI 2581248)

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). (JI 2580228)

If your organization is using Entrust smart credentials, and you set BlackBerry Work to be the authentication delegate, when a user activates the BlackBerry UEM Client, and the Certificate Required message displays, after the user taps Next, the certificates are not shared with the BlackBerry UEM Client and BlackBerry Work stops responding. (JI 2579402)

**Workaround:** Restart BlackBerry Work.

If your organization is using Entrust smart credentials on iOS, if you deactivate a device, the certificates still display as being imported on the Profiles screen. (JI 2569249)

Users might not be able to authenticate with websites or email servers using Entrust smart credentials on Samsung KNOX 3.1 devices. (JI 2567516)

After an iOS user imports a certificate, the user is taken through the import process again. (JI 2538500)

When you use a Work space only activation type to activate an Android 8.0 device and you configure a Wi-Fi profile in BlackBerry UEM, the device user might not be able to connect to a Wi-Fi network. (JI 2371987)

**Workaround:** In your organization's IT policy, select the "Allow changing Wi-Fi settings" option. Note that this issue is fixed in Android 8.1.

When you use a Samsung KNOX activation profile to activate an Android device and you select the "Google Play app management for Samsung KNOX Workspace devices" option, the device will not activate and a Google Play services error will display. For more information, visit <http://support.blackberry.com/kb/> to read article KB469178. (JI 2343363)

On a Samsung KNOX device, required BlackBerry UEM hosted apps might not display in the "Installed" section when the user opens Google Play on the device, even if they are actually installed. (JI 2251895)

If a user deletes BlackBerry Access from their device, and then generate access keys for another user in BlackBerry UEM Self-Service, if the user uses those keys when re-installing BlackBerry Access on their device, you can't assign any app configurations to the user's device. (JI 2237117)

You cannot re-activate a macOS device if you remove the activation profile on the device. (JI 2226652)

The BlackBerry UEM Client is not automatically updated for devices that use an Apple VPP account when the VPP account setting "Automatically update the app when a new version is available" is enabled in BlackBerry UEM. (JI 2197631)

### **Management console known issues**

In a BlackBerry UEM and BES5 integrated environment, if you delete a BlackBerry OS user from the BlackBerry Administration Service without selecting the "Delete the user and remove the BlackBerry information from the user's mail system" option, and then you add the same user to BlackBerry UEM and activate a BlackBerry OS device for the user, the BlackBerry OS device information does not display in the BlackBerry UEM management console.

\* If a user has uploaded a certificate for a BlackBerry Dynamics-enabled device in the self-service portal, when you delete the user in the management console, the certificate that is associated with the BlackBerry Dynamics-enabled device remains in the database. (JI 2653816)

\* When you try to delete a user that has a certificate assigned to them, an error displays. (JI 2653782)

\* The BlackBerry Dynamics Launcher might not display on devices for users that are assigned the "Feature – BlackBerry App Store". (JI 2654521)

**Workaround:** Create a new enterprise connectivity profile for the users, and remove the "Feature – BlackBerry App Store".

\* You might not be able to update the app configuration for BlackBerry Work. (JI 2651336)

**Workaround:** Recreate the app configuration.

\* On the Users > Apple DEP devices page, if you select the top checkbox to select all of the devices in the list, only the devices that are visible on the screen are selected. (JI 2646995)

\* If you open the BlackBerry Connect app, click on an app configuration, click the Server Configuration tab, remove the information in the Connect Server Hosts field and click Save, when you click on the app configuration again, the information still displays. (JI 2646430)

\* When you are on the Managed device users page, if you select one user, and click Send activation email, the console displays a notification that the email was sent but the recipient does not receive the activation email. (JI 2646269)

\* When you navigate to Settings > BlackBerry Dynamics > Clusters or Direct Connect, the BlackBerry Proxy instance might not display. (JI 2646268)

**Workaround:** Upgrade the BlackBerry Connectivity Node to the latest version.

\* If you add an iOS and Android version of an app and both apps have the same name, only one of the apps displays on the App rankings page. (JI 2645646)

\* On the Personal apps page, some apps for Windows devices might display with no name and a null version number. (JI 2643915)

\* When you try to assign an OTP token to an LDAP user, an error message displays. (JI 2642308)

\* When you create a local or directory user that does not have an email address, a variable of <tenantID>/<username> is used in place of the email address. The forward slash (/) causes user activation to fail. (JI 2641669)



**Workaround:** Edit the user to change the forward slash to a backward slash (\).

**Workaround:** Turn off the certificate authority chain in the OpenTrust server when you create profiles.

\* On the App groups page, if you click the number in the Applied users column, only the first user displays. (JI 2641005)

**Workaround:** To view all of the users, after you click the number in the Applied users column, click the Assigned to users tab.

\* If you are using the BlackBerry Gatekeeping Service, Android devices that use the Gmail client are not automatically added to the list of allowed devices. (JI 2640686)

**Workaround:** Manually allow the quarantined devices in Microsoft Exchange ActiveSync.

\* When you create a BlackBerry Dynamics connectivity profile it does not include the BlackBerry Cloud Enterprise Services app server. (JI 2640613)

**Workaround:** Copy the default BlackBerry Dynamics connectivity profile when you need to create a profile that includes BlackBerry Cloud Enterprise Services.

\* If you are using Internet Explorer to view the management console, when you navigate to Settings > BlackBerry AtHoc > User sync settings and click Sync now, the progress bar does not advance even though the sync completes successfully. (JI 2640605)

**Workaround:** Use Google Chrome to view the console.

\* When you have a BlackBerry Connectivity Node configured, if you add a BlackBerry Dynamics connectivity profile, and in the BlackBerry Connectivity Node console (<http://localhost:8088>), you click General settings > BlackBerry Router and proxy and select the Enable HTTP proxy checkbox and configure the proxy settings, the proxy might not be used. (JI 2638371)

\* If you are configuring Android Enterprise, when you accept permissions for the default apps, the console might stop responding. (JI 2637634)

**Workaround:** Open a new browser window and add the default apps manually.

\* Future licenses do not display a start date or expiration date on the Licensing Summary screen. (JI 2636721)

\* When you add an app and you select the 'Internal BlackBerry Dynamics app entitlements' option, if you try to upload a png or jpeg image for the app from your desktop an error occurs. (JI 2636029)

**Workaround:** Use the 'Upload image using URL' option, or you can upload an svg image using the 'Upload image from desktop' option.

\* If you assign the "First" BlackBerry Cluster to the default BlackBerry Connectivity profile, and you navigate to Settings > BlackBerry Dynamics > Clusters, create an empty "Second" cluster, and reassign the server that is associated with the First cluster to the second cluster and click Save, an error message displays. The Enabled for activation option also is cleared for the First cluster. (JI 2635165)

**Workaround:** Re-select the 'Enabled for activation' option.

\* You cannot remove Microsoft Active Directory users who have activated devices that use BBM Enterprise. (JI 2633996)

**Workaround:** Deactivate the device, remove the BBM Enterprise service from the user and remove the user from BlackBerry UEM.

\* When you click the Renew button twice on the user credential profile page, an error message displays. (JI 2633794)

\* When you navigate to Settings > BlackBerry Dynamics > Clusters and rename the 'First cluster, if you install a second unit of scale, on the BlackBerry Dynamics Connectivity profile, in the App servers section, the cluster name is blank. (JI 2632061)

\* When you create a certificate mapping profile, if you select the Specified apps option, click +, search for apps, select multiple apps that the search returned and click add, more apps might be added to the list than those that you selected. (JI 2627085)

\* If you change the settings of a SCEP profile or user credential profile based on a native keystore, users are not prompted to enroll the certificates again and only new certificates receive the updated settings. (JI 2626894)

**Workaround:** Delete the profile and create and assign new one to apply the new settings.

\* There is no indication in the management console that a device had failed Android SafetyNet attestation. (JI 2626552)

\* When you are creating a user credential profile, if you select the 'Native keystore' option in the Certification authority connection list, the bottom of the page is cut off. (JI 2623712)

\* When the browser does not have a certificate, or you import the wrong certificate, or the certificate is expired a timeout page displays instead of an error message. (JI 2621218)

\* When you use invalid user credentials when you are configuring PKI for BlackBerry Dynamics, a generic message displays: "Service Temporarily Unavailable." (JI 2572909)

In the BlackBerry Dynamics profile, if you upload a list that has more than 10000 banned passwords, it is truncated at 10000 passwords. (JI 2511201)

When you are using the Advanced view in the management console, the device details page displays the incorrect Total internal storage amount for devices. (JI 2376060)

When you synchronize a large company directory, the synchronization might stop responding. (JI 2228017)

When you create an IT policy for Android devices, the "Force the device and work space passwords to be different" rule implies that the personal and work space passwords must be different. However the passwords can be the same, although they are separate. (JI 2206856)

You cannot update the version of an app in the BlackBerry UEM console before the newer version of the app is available in Google Play. (JI 2203775)

**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.

When you delete a user that is enable to use BlackBerry Workspaces, the message that displays is misleading. (JI 1657607)

**Workaround:** Log in to the console as a BlackBerry Workspaces Organization administrator who has an email address, remove the BlackBerry Workspaces service from the user, and then delete the user.

### **BlackBerry UEM Core known issues**

\* The BlackBerry UEM Core might not shut down in a timely manner. (JI 2609643)

**Workaround:** In Windows Task Manager, stop the BlackBerry UEM Core service.

### **UEM Self-Service known issues**

The expiration period for access keys generated in UEM Self-Service is 24 hours instead of 30 days. (JI 1659057)

### **Documentation known issues**

\* When you try to access pages in the documentation website [docs.blackberry.com](https://docs.blackberry.com), you might receive page not found errors intermittently.

**Workaround:** Clear you browser cache and try again, or use a browser in incognito mode.

# Maintenance releases of the BlackBerry Connectivity app

The BlackBerry Connectivity app is required for devices to use the BlackBerry Secure Connect Plus feature in BlackBerry UEM. Maintenance releases of the app might occur between BlackBerry UEM releases. To view the Release Notes for the latest maintenance releases of the app, visit <http://help.blackberry.com/en/blackberry-connectivity/current/>.

For more information about enabling and using BlackBerry Secure Connect Plus, see "Using enterprise connectivity and BlackBerry Secure Connect Plus for connections to work resources" in the Administration content.

# Legal notice

©2018 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Android, Google, Google Play, Pixel, and SafetyNet are trademarks of Google Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. AirDrop and Safari are trademarks of Apple Inc. Entrust is a trademark of Entrust, Inc. Microsoft, Intune, Windows 10, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Bluetooth is a trademark of Bluetooth SIG. KNOX and Samsung KNOX are trademarks of Samsung Electronics Co., Ltd. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY

EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES 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  
200 Bath Road  
Slough, Berkshire SL1 3XE  
United Kingdom

Published in Canada