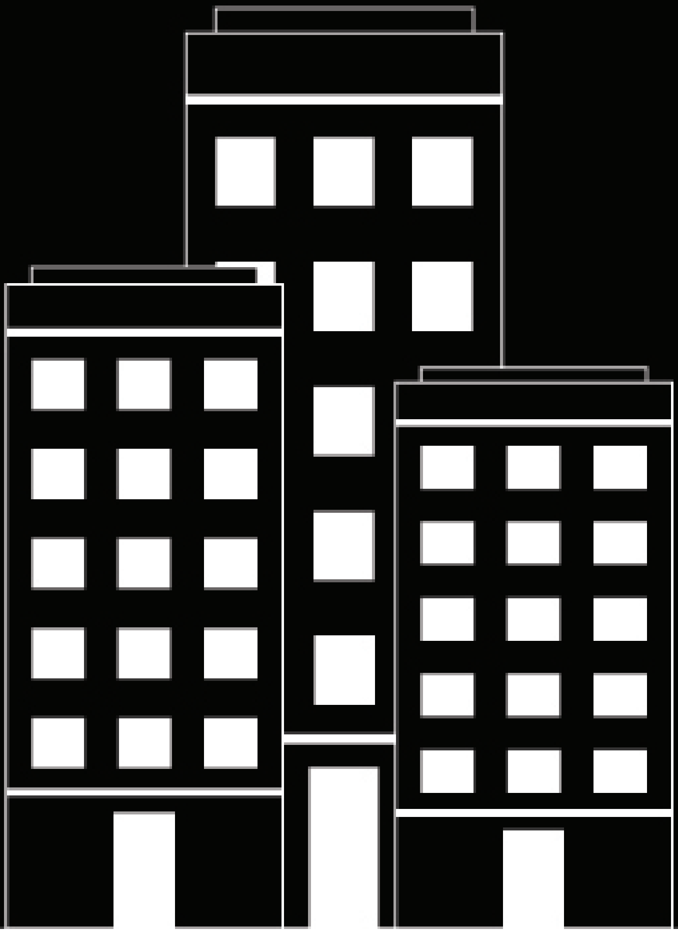

BlackBerry UEM

Release Notes

12.19

Contents

BlackBerry UEM 12.19 and UEM Cloud (November 2023) Release Notes

What's new in this release?

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

Critical issue advisories for UEM

See the following Critical Issue Advisory Knowledge Base articles for information about key issues that may impact your UEM environment, as well as workarounds and possible resolutions: and the

- UEM Critical Issue Advisories
- BlackBerry Enterprise Mobility Server Critical Issue Advisories

Installing UEM on-premises

You can use the setup application to install UEM version 12.19 or to upgrade from UEM 12.17 or 12.18.x. When you upgrade the software, the setup application stops and starts all of the UEM services for you and backs up the database by default.

Considerations for Android Management activation types

This release introduces the following new activation types that support the Android Management API:

- Work and personal - full control (Android Management fully managed device with work profile)
- Work and personal - user privacy (Android Management with work profile)
- Work space only (Android Management fully managed device)

Note the following considerations for the new Android Management activation types:

UEM feature	Considerations
IT policy password considerations	• For devices with the Work and personal - full control activation type, the device and the work space use the Password requirements setting. • For devices with the Work space only activation type, the work space uses the Password requirements setting. • For devices with the Work and personal - user privacy activation type: • Devices with Android OS 12 and later use the Password complexity setting. • Devices with Android OS 11 and earlier use the Password requirements setting. • The work space uses the Password requirements setting.
Activation	• QR codes for Android Management activations expire after each use. • Activating Android Management devices using managed Google Play accounts is supported (see Configuring BlackBerry UEM to support Android Management devices). Activating devices with managed Google domain configurations are not currently supported. • UEM Client log information is not accessible during device activation of the Work and personal - full control and Work space only activation types. For activation failures for these activation types, you can review the UEM server core logs.
Activation profile	You must create separate activation profiles for Android Enterprise and Android Management. If Android Enterprise and Android Management activation types are specified in the same profile, the Android Management type will take precedence, even if it is ranked lower than Android Enterprise. Only the password and activation information for the Android Management activation type will be embedded in the QR code.
App management	Currently, only Google Play apps can be pushed to Android Management devices.
Certificates	• For native Android apps, only CA certificate profiles are currently supported. Shared certificate, user credential, and SCEP profiles are not currently supported. • For BlackBerry Dynamics apps, certificate support is the same as for Android Enterprise activation types, however, Purebred certificates are not currently supported.
Certificate mapping profile	Certificate mapping profiles are not currently supported for devices with Android Management activation types.

UEM feature	Considerations
CylancePROTECT Mobile for BlackBerry UEM	• Any settings in the management console related to CylancePROTECT Mobile for UEM are currently not applicable to devices with Android Management activation types. • Compliance rules for CylancePROTECT Mobile for BlackBerry UEM features are not currently supported for devices with Android Management activation types.
Device commands	• Remove device command: Deletes work space data for the Work and personal - user privacy activation type and deletes all device data for the Work and personal - full control and Work space only activation types. • Lock device command: For devices with the Work and personal - user privacy and Work and personal - full control activation types, if one lock is enabled, the device is locked. If one lock is not enabled, only the work space is locked. For devices with the Work space only activation type, the device is locked. • Specify device password and lock command: Sets the work space password for devices with the Work and personal - user privacy and Work and personal - full control activation types. For devices with the Work space only activation type, this command sets the device password. • Delete all device data: Deleting data from an SD card, factory reset protection, and preserving a device's data plan are not supported for devices with Android Management activation types.
Device profile	Wallpaper images are not currently supported for devices with Android Management activation types.
Device SR requirements profile	Only OS update is supported for devices with Android Management activation types. Suspending OS updates and automatic app updates are not currently supported.
Email profile	• Samsung email is not currently supported for devices with Android Management activation types, as the Knox API is not currently supported. • BlackBerry Work is supported.
Enterprise connectivity profile	• Enterprise connectivity profiles and BlackBerry Secure Connect Plus are not currently supported for devices with Android Management activation types. • An assigned enterprise connectivity profile may display in the user’s details in the management console even though the profile is not currently supported for Android Management.
Factory reset protection profile	Only the “Enable and Specify Google account credentials when the device is reset to factory settings” option is supported for devices with Android Management activation types.

UEM feature	Considerations
Private apps	When both Android Enterprise and Android Management are configured in your UEM environment, you can publish private apps for Android Management devices only. In this scenario, to send private apps to Android Enterprise and Android Management devices, from the Google Play console, publish the app and add both Android Enterprise and Android Management org IDs. For more information, see Managed Google Play Help: Publish private apps from the Play Console. After you complete this task, in the UEM management console (Apps > add an app > Google Play), you can search for the apps and add them to UEM.
UEM Self-Service	If a user's activation profile contains ranked Android Enterprise and Android Management activation types, regardless of ranking, the Android Management activation type is used. The QR code generated by UEM Self-Service will use the Android Management activation type.
Wi-Fi profile	Only the following settings are currently supported for devices with Android Management activation types: • SSID • Security type: Personal • Personal security type: WPA-Personal/WPA2-Personal • Preshared key • Security type: Enterprise • Authentication protocol: PEAP + Outer identify for PEAP • Username • Password • Certificate common names expected from authentication server • Type of certificate linking • CA certificate profile

Fixed issues in UEM 12.19 and UEM Cloud

UEM 12.19 Quick Fix 8 (August 2024)

Management console fixed issues

If you tried to add certain Android APKs that were published to Google Play to UEM as internal app, the APK file could not be verified. (EMM-156847)
Additional logging has been added for calls to Google APIs for publishing hosted applications. (EMM-156841)
In specific circumstances, opening an app group resulted in an error indicating that the app group details could not be retrieved, and the app group did not open as expected. (EMM-156584)

User, device, and app management fixed issues

When BlackBerry Secure Connect Plus made an authorization check for a device, if the checked failed, it would not attempt another authorization check for at least one hour. (EMM-156726)

UEM 12.19 Quick Fix 6 (July 2024)

Upgrade fixed issues

If you tried to upgrade to UEM 12.19, the upgrade process failed if JRE 8 was installed on the computer after you installed JRE 17, which is required for UEM 12.19 and later. Installing JRE 8 for other purposes caused issues with the path variable. (EMM-154349)

Management console fixed issues

You might not have been able to log in to the management console if you enabled OCSP certificate-based authentication. (EMM-156040, EMM-156067)

User, device, and app management fixed issues

If you used the UEM REST API Delete user command and specified users with active devices, the users' data might have been deleted from the BlackBerry Infrastructure and from partner systems such as Google and Apple, but the user was not removed from the UEM environment. (EMM-156426)

UEM 12.19 Quick Fix 7 (July 2024)

Management console fixed issues

The "Allow Factory Reset" option in the Knox Service Plugin profile was labelled incorrectly. It has been fixed to read "Block Factory Reset". (EMM-155439)

User, device, and app management fixed issues

If you configured the UCM Plugin configurations (premium) and VPN profiles (premium) settings in a Knox Service Plugin profile and assigned the profile to users, the Delete all device data command did not complete successfully when it was sent to users that were assigned the profile. (EMM-156118)

Under certain circumstances, you might not have been able to create a UEM recovery account due to the UEM Configuration Tool expecting a tenant id value of 1. (SDS-1333)

UEM 12.19 Quick Fix 6 (July 2024)

Upgrade fixed issues

If you tried to upgrade to UEM 12.19, the upgrade process failed if JRE 8 was installed on the computer after you installed JRE 17, which is required for UEM 12.19 and later. Installing JRE 8 for other purposes caused issues with the path variable. (EMM-154349)

Management console fixed issues

You might not have been able to log in to the management console if you enabled OCSP certificate-based authentication. (EMM-156040, EMM-156067)

User, device, and app management fixed issues

If you used the UEM REST API Delete user command and specified users with active devices, the users' data might have been deleted from the BlackBerry Infrastructure and from partner systems such as Google and Apple, but the user was not removed from the UEM environment. (EMM-156426)

UEM 12.19 Quick Fix 5 (June 2024)

User, device, and app management fixed issues

If you used the BlackBerry Web Services REST API to send a command to a device to wipe data but preserve the device's eSIM data, the eSIM data was not preserved as expected. (EMM-156093)

UEM 12.19 Quick Fix 4 (May 2024)

This Quick Fix release includes the fixes from any previous QF release.

User, device, and app management fixed issues

If you associated a user credential profile with a VPN profile and assigned the VPN profile to users, the VPN profile was not applied to the users as expected. (EMM-156008)

UEM now uses the cRLSign bit field to verify that a certificate is trusted before checking the CRL. (EMM-155996)

This release includes the following changes to IT policy rules for Android password complexity:

- The Android Global Password complexity IT policy rule now applies only to devices with Android OS 12 or later with a user privacy activation type (Android Enterprise and Android Management).
- The Android Global Password requirements IT policy rule now applies to full control and work space only activation types (Android Enterprise and Android Management), and to user privacy activation types (Android Enterprise and Android Management) on devices with Android 11 only.
- The Password complexity IT policy rule in the Android Work profile section is no longer applicable as of UEM Client version 12.44.x.
- The Password requirements rule in the Work profile section now applies to all Android activation types.

Note that the tooltip text to clarify the changes for these rules will not be visible in the UI until the next IT policy pack is released (currently planned for June 2024). (EMM-155761)

The BlackBerry Dynamics profile includes a new setting, Start conditional access enrollment after authentication broker is installed, that allows you to delay Entra ID conditional access enrollment for a user until the Microsoft Authenticator app is installed on the user’s device. (EMM-154216)

After upgrading UEM, the UEM root certificate was renewed even though it had not expired. As a result, some Samsung devices did not activate with UEM because the server certificate could not be validated. (EMM-154119)

The following options have been added to the BlackBerry Dynamics profile:

- Enable Dynamics Launcher in UEM Client: This setting specifies whether the BlackBerry Dynamics Launcher icon appears in the UEM Client.
- Enable Dynamics Launcher first time setup: This setting specifies whether the tutorial appears when the BlackBerry Dynamics Launcher appears for the first time in the UEM Client.

(EMM-153611)

UEM 12.19 Quick Fix 3 and UEM Cloud (April 2024)

This Quick Fix release includes the fixes from any previous QF release.

User, device, and app management fixed issues

This release includes the following changes (the IT policy changes were also made available in the latest IT policy pack):

- The "Allow marketplace apps" IT policy rule has been added to allow you to control whether users can install marketplace apps. This rule is supported for iOS 17.4 and later.
- The functionality of the following iOS IT policy rules now extend to marketplace apps: Allow installing apps (supervised only), Allow removing apps (supervised only).
- The functionality of the following iOS compliance rules now extend to marketplace apps: Show only allowed apps on the device, Restricted app is installed.

(EMM-155942)

When you tried to save a change to an IT policy that was assigned to a device group, the change could not be saved. (EMM-155566)

In a UEM Cloud environment, the BlackBerry Cloud Connector could not synchronize more than 1500 users for an LDAP directory group. This issue is resolved in this QF with a new release of the BlackBerry Cloud Connector. Use the setup application for the BlackBerry Connectivity Node (Settings > External integration > BlackBerry Connectivity Node setup) to update the BlackBerry Cloud Connector. (EMM-155301)
You could not change the disposition of an app group that was assigned to a user or device group. (EMM-154392)
When you assigned an app or app group to a user group, then viewed the group from the user view (navigate to the user then click the group), the disposition of the app or app group was listed as "Undefined" instead of the actual disposition setting. The same issue occurred if you assigned the app or app group to a device group and then opened the device group. (EMM-154391)

UEM 12.19 Quick Fix 2 (March 2024)

This Quick Fix release includes the fixes from any previous QF release.

Installation or upgrade fixed issues

After completing a scripted install of UEM, you could not log in to the management console. (EMM-155491)

User, device, and app management fixed issues

If a user was assigned an IT policy with "Enable activation lock" enabled for iOS devices, and the device had a null MEID value, UEM was not able to apply profiles or commands to the device. (EMM-155671)
When a user activated a device with an Android Enterprise activation type, an issue with Google API calls might have caused a delay in pushing assigned apps to the device. (EMM-155385)
Previously, if a user tried to activate an Apple DEP device and their device did not have a required OS version, the activation failed. The DEP activation process has been improved to prompt the user to upgrade the OS, if required. (EMM-153864)

UEM 12.19 Quick Fix 1 and UEM Cloud (January 2024)

Installation or upgrade fixed issues

If you tried to upgrade UEM on-premises from version 12.18 to 12.19 using the command line, the upgrade did not complete successfully. (EMM-154989)

Management console fixed issues

In a UEM Cloud environment, if you navigated to the Org Connect section of the management console, an error message displayed indicating that you should verify that your organization uses BBM Enterprise, and you could not access the Org Connect UI. (EMM-155126)
Devices with activation lock enabled might not have displayed as expected in the Users > Apple Activation Lock screen. (EMM-154070)

User, device, and app management fixed issues

In a UEM on-premises environment, when you integrated UEM with a Google domain to manage Chrome OS devices, UEM sent an incorrect ID in REST calls to Google, resulting in 400 errors. (EMM-155274)
Due to a specific error that could occur during the activation of an Android device, the Google Play device policy might not have been set correctly. As a result, the device could encounter issues with app deployment or other features. (EMM-155259)
After an OS update was installed on an iOS device, UEM might have continued to send update OS commands. (EMM-155104)
Hardware attestation failed on Android devices if certificate data was not recognized by UEM. (EMM-154980)
When a REST API was used to update iOS devices, some available updates for iOS devices were missing. (EMM-154517)
Shared iPad devices did not support BlackBerry Secure Connect Plus. (EMM-154285)

UEM on-premises 12.19 and UEM Cloud (October 2023)

Management console fixed issues

The RSR version was not displayed in UEM after an iOS device was updated to the RSR version. (EMA-17723)
Administrators could not delete a certificate from the CA certificate profile page. (EMM-153265)
The IT policy tooltip for "Allow screenshots in the work profile to be stored in the personal profile" was updated to indicate that screenshots must be stored in the personal profile if the option is selected. (EMM-152026)
If a SIEM connector was configured with TLS settings that did not match the syslog server settings, scheduled tasks did not run. (EMM-151864)
After you removed Apple VPP apps from a device and unassigned them from the user, the license consumption counts were not updated in the management console. (EMM-151299)

User, device, and app management fixed issues

The work profile was not removed or the device was not reset to factory default settings if the Remove device command was sent while the device was offline. (EMA-17733)
SCEP enrollment was not completed during activation of Android devices when the CMS Algorithm Identifier Protection attribute was used. (EMA-17636)
Wi-Fi profiles with the Enterprise security type were not applied to devices because the root CA or domain name were not applied to users devices. (EMM-153133)
BlackBerry Work did not activate automatically when it was set as the primary authentication delegate on an iOS DEP device. (EMM-152855)
The activation password expiry date was not displayed correctly in UEM Self-Service when the language was set to French. (EMM-152389)

App shortcuts were displayed in the personal apps list in UEM after they were configured to appear in the BlackBerry Dynamics Launcher. (EMM-152316)
After you upgraded from BlackBerry UEM 12.17.1(a) to 12.18, device groups that include RSR versions were not updated automatically. (EMM-152033)
For iOS devices, RSR versions might have been included in device groups that were intended to filter for a specific version and earlier or later versions. (EMM-152028)
Users could not edit notification permissions for apps on Samsung devices running Android 13. (EMM-151936)

Known issues in UEM 12.19 and UEM Cloud (November 2023)

Management console known issues

If you assign an app group to a user or group, when you edit that user or group you cannot change the disposition of the app group. (EMM-154392) **Workaround**: Remove the app group from the user or group, then create and assign a new app group with the desired disposition.
If you activate both Android Enterprise and Android Management devices, then remove the Android Management connection from UEM, the console will display an incorrect count of the devices that will be removed. The count includes both Android Enterprise and Android Management devices. Only Android Management devices will be removed. (EMM-154081)
In a UEM Cloud environment, if you turn on "Send SMS/MMS logs to the BlackBerry Connectivity Node" or "Send phone logs to the BlackBerry Connectivity Node" in an IT policy and the BlackBerry Connectivity Node is not installed, the following error displays: "An error was encountered. The profile could not be created." The error message should indicate that the settings could not be enabled because the BlackBerry Connectivity Node is not installed. (EMM-154049)
In the Device tab of an org unit, if you try to configure a scheduled reboot, you cannot save the configuration unless you update all three sub-fields. (EMM-153890)
When you view the device details for a user with more than one SIM, the expand and collapse arrow does not display as expected for SIM 1. You can still expand and collapse the SIM details. (EMM-153727)
Entra ID directory synchronization reports do not display changes to users' group membership after the report runs. (EMM-153691)
If a user deactivates a device with an Android Management activation type from the device settings, the device still displays as activated in the management console. (EMM-153468)
When you send the Delete only work data command to an iOS device that is activated with User privacy, the request times out and an error message is displayed. (EMM-153457) **Workaround**: Use the Remove device command.
When you assign an IT policy to devices that are running Windows 10 21H2, a "Command Failed" error might be displayed when you view the device actions and the IT policy is not applied. (EMM-151905)
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)
The value of the variable %ComplianceDynamicsEnforcementActionWithDescription% does not display as expected in compliance notification emails that are sent to users. (EMM-151056)
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)

When compliance override policies are applied, UEM might not send the compliance violation status to Entra ID conditional access. (EMM-148486)

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)

When you are configuring Entra ID 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 Entra ID Conditional Access page, and complete the configuration steps again.

User, device, and app management known issues

In UEM 12.18 and earlier environments, if you enabled the "Allow wearables" setting to allow an Apple Watch to synchronize with the BlackBerry Work app and then upgraded to UEM 12.19, the Apple Watch will no longer synchronize with BlackBerry Work. (EMM-154314)

Workaround: In the BlackBerry Dynamics profile settings, disable the "Allow wearables" setting and enable the “Allow WatchOS apps" setting to allow Apple Watch synchronization with BlackBerry Work.

Samsung devices that are activated with Android Enterprise Work space only and are assigned an Enterprise connectivity profile cannot send or receive SMS or MMS messages. (EMM-154287)

Workaround: In the Enterprise connectivity profile settings, on the Android tab, select Container-wide VPN and add the com.android.mms.service and com.google.android.apps.messaging apps to the list of apps restricted from using BlackBerry Secure Connect Plus.

If a Knox Service Plugin (KSP) policy is set to disable factory reset on a device and you send 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)

In dark site environments, when activating a Samsung Galaxy S 20 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)

On Android devices, when you open the Work apps menu from the BlackBerry Dynamics Launcher, the app list loads, but an error message is displayed at the bottom of the screen. (EMM-151977)

Chrome OS devices will not synchronize with UEM if they are in an org unit that has no child org units. (EMM-150375)

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

If you don't configure an app server for Entra ID 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.

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.

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.
During the Entra ID 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.

BlackBerry Connectivity Release Notes

The BlackBerry Connectivity app is required for devices to use the BlackBerry Secure Connect Plus feature in BlackBerry UEM. For more information about enabling and using BlackBerry Secure Connect Plus, see Using BlackBerry Secure Connect Plus for connections to work resources. The BlackBerry Connectivity app supports TLS 1.2 and DTLS 1.0.

The following changes are new in the latest release of the BlackBerry Connectivity app:

Platform	Latest version	What's new
Android	1.25.0.990	• New fixed issues. See Fixed issues for BlackBerry Connectivity. • Support for features in the UEM 12.20 release.
iOS	1.0.25.490	Adds BlackBerry Secure Connect Plus connectivity support for shared iPad groups in the UEM 12.19 Quick Fix 1 release.

Fixed issues for BlackBerry Connectivity

BlackBerry Connectivity for Android

On some Android 14 devices, the BlackBerry Connectivity app could not connect as expected over the Wi-Fi network. (BSCP-995)
After upgrading to Android 14, the BlackBerry Connectivity app might have stopped responding and required multiple device restarts to work as expected. (BSCP-964)
The BlackBerry Connectivity app repeatedly attempted to connect to the BlackBerry Secure Connect Plus server after the device had been removed from BlackBerry UEM. (BSCP-832)
The BlackBerry Connectivity app stopped responding if the device had been removed from BlackBerry UEM. (BSCP-831)
Downloads and updates for work apps got stuck at the "Download pending" status. (BSCP-823)

BlackBerry Connectivity for iOS

The BlackBerry Connectivity app continued to show a Connected state even though it had been disconnected. (BSCP-837)
The BlackBerry Connectivity app repeatedly attempted to connect to the BlackBerry Secure Connect Plus server after the device had been removed from BlackBerry UEM. (BSCP-832)
The BlackBerry Connectivity app stopped responding if the device had been removed from BlackBerry UEM. (BSCP-831)

The BlackBerry Secure Connect Plus connection might have been intermittently lost due to dropped packets when the work queue was full. The secure tunnel connection was not automatically re-established. (BSCP-793)

Known issues for BlackBerry Connectivity

BlackBerry Connectivity for Android

On Samsung devices activated with the Work space only (Android Enterprise fully managed device) activation type, you cannot send or receive MMS messages when container-wide VPN is enabled. (BSCP-824)

BlackBerry Connectivity for iOS

When a user tries to upgrade from a previous version of the app to the latest version available in the App Store, the upgrade might not complete successfully due to a known issue in the iOS software. **Workaround:** Uninstall the app that is currently on the device, then install the latest version that is available in the App Store.
When trying to upgrade the BlackBerry Connectivity app on devices running iOS 13, the app update stalls and might not complete successfully if the device has a secure tunnel connection established. (BSCP-808) **Workaround**: Before you update the BlackBerry Connectivity app, disconnect the secure tunnel connection. After you update the app, check the app to verify that the connection is re-established.
If an enterprise connectivity profile with per-app VPN configured is assigned to an iOS device with the User privacy - User enrollment activation type, the per-app VPN connection cannot be established. (BSCP-801)

Legal notice

Patents, as applicable, identified at: www.blackberry.com/patents.

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, MERCHANTABLE QUALITY, 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
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada