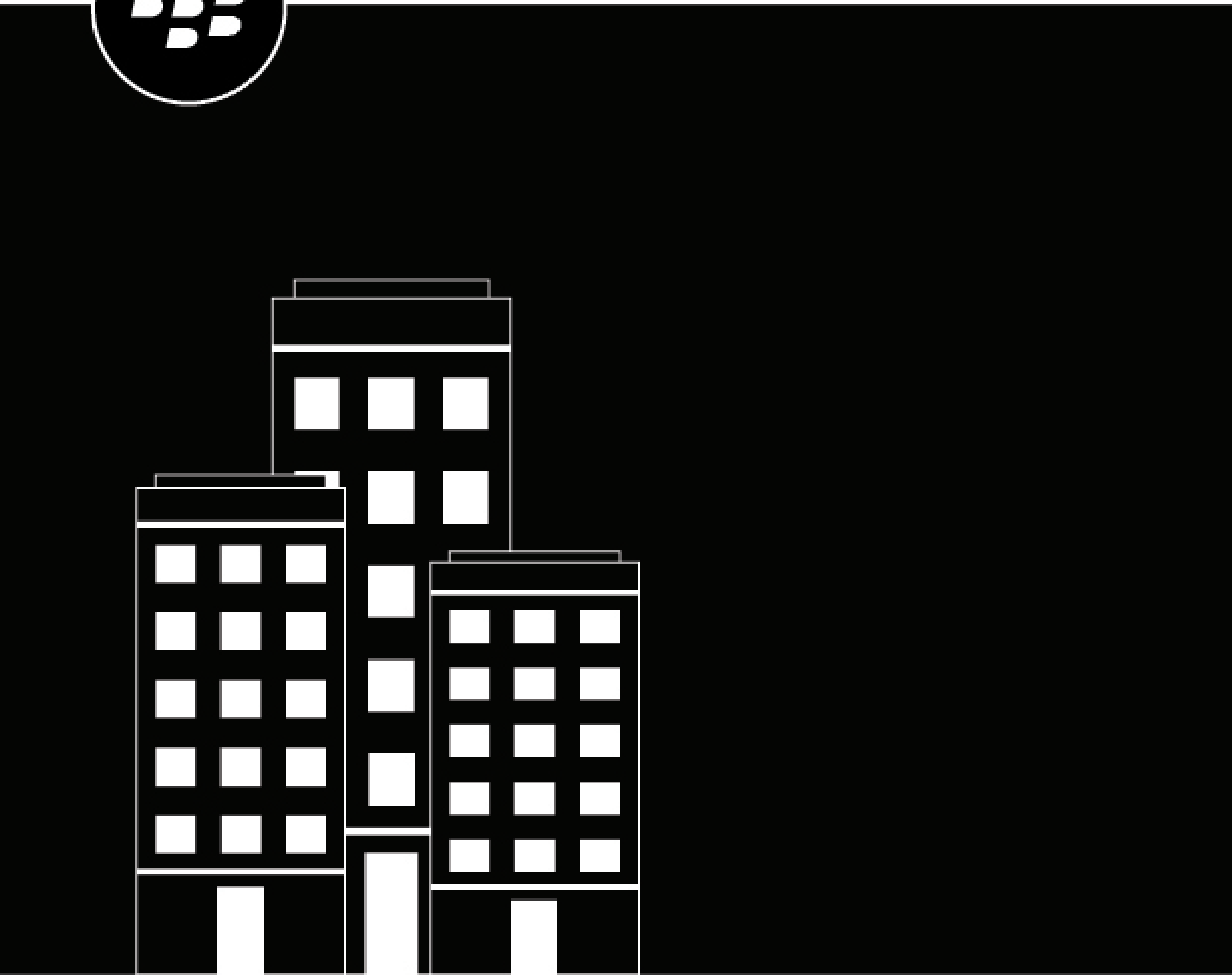

BlackBerry UEM Client for Android

Release Notes

12.45.0.158273

Contents

What's new in the BlackBerry UEM Client for Android

What's New in the BlackBerry UEM Client for Android 12.45.0.158273

The previous release of the UEM Client for Android introduced a change for enterprise connectivity configured for container wide VPN (see "Enterprise connectivity enhancement" for version 12.45.0.158224). This release modifies the described behavior so that it occurs only if the user is assigned an Intercede user credential profile.

In the previous release, if you did not want the UEM Client to route traffic through BlackBerry Secure Connect Plus, or if you used the UEM Client as the authentication delegate for BlackBerry Dynamics apps, you had to add the package ID of the UEM Client to the restricted apps list in the assigned enterprise connectivity profile. With the changes made in this release, you no longer need to add the package ID of the UEM Client to the restricted apps list, but it is still recommended to add the UEM Client to the restricted apps list if you do not want traffic to go through BlackBerry Secure Connect Plus.

For more information, and to verify that VPN traffic is not blocked by firewall or proxy settings, see KB140552.

What's New in the BlackBerry UEM Client for Android 12.45.0.158224

Enterprise connectivity enhancement: If you've enabled BlackBerry Secure Connect Plus for your organization's Android devices, and you selected "Container wide VPN" in the assigned enterprise connectivity profile, by default the BlackBerry UEM Client will route device-wide VPN traffic through BlackBerry Secure Connect Plus to UEM. If you do not want the UEM Client to route traffic through BlackBerry Secure Connect Plus, or if you use the UEM Client as the authentication delegate for BlackBerry Dynamics apps, add the package ID of the UEM Client to the restricted apps list in the assigned enterprise connectivity profile.

This change does not impact enterprise connectivity profiles where BlackBerry Secure Connect Plus is configured for "Per-app VPN", unless the package ID of the UEM Client is added to the list of apps that are allowed to use enterprise connectivity.

Note that if your organization uses BlackBerry Dynamics apps, it is recommended that you restrict the apps from using BlackBerry Secure Connect Plus. For more information, see Android: Enterprise connectivity profile settings.

What's New in the BlackBerry UEM Client for Android 12.45.0.158217

This hotfix release addresses key fixes. For more information, see BlackBerry UEM Client for Android fixed issues.

What's New in the BlackBerry UEM Client for Android 12.45.0.158182

- **Support for Android 15**: The UEM Client now supports devices running Android 15, including devices with Samsung Knox.
- **Derived credentials**: Users can now scan an Intercede MyID QR code using the UEM Client (Profiles > Import certificates) to activate with MyID and download derived credentials certificates. Administrators can configure the profile to download the certificates from MyID to the device’s BlackBerry Dynamics keystore and, optionally, the device’s built-in native key chain. This feature requires BlackBerry UEM server 12.21.
- **Allow Circle to Search functionality**: The "Allow Circle to Search" IT policy rule allows administrators to control whether the Circle to Search functionality is enabled in the work profile. The rule is enabled by default and applies to devices running Android 15 or later. This feature requires BlackBerry UEM server 12.21.
- **UI changes in the UEM Client**:
  - The "Password and biometrics" section in the Settings menu is hidden if the administrator selected the "Do not require password" option for Android device in the BlackBerry Dynamics profile.

    - The "Assigned IT policies" menu is hidden in the UEM Client home screen if the device is activated with the User privacy activation type.
- **Changes to IT policy rules**: The "Allow screenshots in the work profile to be stored in the personal profile" IT policy rule is not supported on devices running Android 15 or later.

What's New in the BlackBerry UEM Client for Android 12.44.0.158016

Fixed an issue where the UEM Client was stuck on the Configuring BlackBerry Dynamics screen during activation if the administrator enabled the "Start conditional access enrollment after the authenticator broker app is installed" option. This affected devices with the Work and personal - full control (Android Enterprise) or Work space only (Android Enterprise) activation types. (EMA-18477)

BlackBerry Dynamics SDK and BlackBerry Dynamics Launcher versions

As of the BlackBerry Dynamics SDK version 13.x, the BlackBerry Dynamics Launcher is fully integrated with the BlackBerry Dynamics SDK.

Version of UEM Client for Android	BlackBerry Dynamics SDK
12.45.0.158273 12.45.0.158224 12.45.0.158217	BlackBerry Dynamics SDK 13.0.2.152
12.45.0.158182	BlackBerry Dynamics SDK 13.0.2.143
12.44.0.158016	• BlackBerry Dynamics SDK 12.1.1.43 • BlackBerry Dynamics Launcher 12.1.590.4

BlackBerry UEM Client for Android fixed issues

Fixed issues in the BlackBerry UEM Client for Android 12.45.0.158217

As a result of Google's deprecation of SafetyNet attestation, the activation process for BlackBerry Dynamics apps was taking up to 5 minutes to complete. (GD-67446)

Fixed issues in the BlackBerry UEM Client for Android 12.45.0.158182

When trying to activate a device with the Work space only (Android Enterprise) activation type in a managed Google account environment, activation was not successful unless the "Allow additional Google accounts" and "Allow adding and removing accounts" options are enabled. (EMA-18647)
On devices activated with the Work space only (Android Enterprise) activation type, the BlackBerry Dynamics Launcher was briefly visible during the conditional access enrollment even though it was not enabled by the administrator. (EMA-18479)
When the "Validate end-user installed certificates" IT policy rule was assigned, the UEM Client also tried to validate certificates from the BlackBerry UEM server which were not end-user installed. In some cases, if the server certificates are received and validated out of their intended order, the validation was not successful and therefore the certificates were not installed. (EMA-18374)

Fixed issues in the BlackBerry UEM Client for Android 12.44.0.158016

During the activation of devices with the Work and personal - full control (Android Enterprise) or Work space only (Android Enterprise) activation types, the UEM Client was stuck on the Configuring BlackBerry Dynamics screen if the administrator enabled the "Start conditional access enrollment after the authenticator broker app is installed" option. (EMA-18477)

Fixed issues in the BlackBerry UEM Client for Android 12.44.0.157998

When there was a certificate fingerprint mismatch for certificates that the server delivered to the UEM Client (for example, trust certificates, root certificates, and SSL certificates), the UEM Client did not include sufficient details to determine the cause of the mismatch. The UEM Client now logs the details to help determine how and when the mismatch occurred and what caused it. (EMA-18303)
If a device password was out of compliance according to the BlackBerry UEM server, the device might not have successfully reported a compliant status to the server if it encountered errors or connectivity issues. (EMA-18038)
When an App Lock mode profile is assigned to a device, the UEM Client was incorrectly displaying extraneous app icons that could not be tapped (for example, the Phone app). (EMA-18016)
When activating a device with the Work space only activation type, the activation completed even though there was a personal Google account on the device which was not allowed. (EMA-17879)

On a device activated with the Work space only (Android Enterprise) activation type in a dark site environment, if the VPN profile was assigned prior to device activation, it was not successfully applied to the VPN application. (EMA-17712)

Fixed issues in the BlackBerry UEM Client for Android 12.44.0.157991

The BlackBerry Dynamics SDK has been updated to version 12.1.0.39 to fix an issue where bad OS compliance data from the BlackBerry UEM server caused the UEM Client to stop responding. (EMA-18398)

BlackBerry UEM Client for Android known issues

When a Samsung device user tries to activate using the Android Enterprise Work and personal - full control activation type, if the screen is locked (for example, the user manually locks the device or the screen times out) or if the device restarts before the activation process completes, when the user unlocks the device, the device is stuck at a blank screen. (EMA-19102)

Workaround: Reset the device from the Android Recovery menu, then activate again and make sure the device does not lock or restart during the activation process.

If you enable Knox DualDAR encryption and select the encryption app in the assigned activation profile, when a Samsung device user tries to activate using the Android Enterprise Work and personal - full control activation type, the activation does not complete as expected. (EMA-19100)

As of UEM Client version 12.45.0.158273, if a user is assigned an Intercede user credential profile and an enterprise connectivity profile with "Container wide VPN" enabled, by default the UEM Client will route container wide VPN traffic through BlackBerry Secure Connect Plus to UEM. If you remove the Intercede user credential profile from a user with an Android Enterprise activation type, the user's device will continue to route VPN traffic through BlackBerry Secure Connect Plus to UEM instead of using a direct connection to UEM. (EMA-19065)

Workaround: Add the UEM Client to the restricted apps list in the enterprise connectivity profile.

As of UEM Client version 12.45.0.158273, if a user is assigned an Intercede user credential profile and an enterprise connectivity profile with "Container wide VPN" enabled, by default the UEM Client will route container wide VPN traffic through BlackBerry Secure Connect Plus to UEM. On Pixel devices, if you assign the Intercede user credential profile to the user after they activate with an Android Enterprise activation type, the user's device will continue to route VPN traffic directly to UEM instead of routing it through BlackBerry Secure Connect Plus. (EMA-19060)

If you assign an IT policy to users with the Password complexity level and Password expiration rules configured for Android devices (work and personal), Samsung devices with Android 15 or later and the "Work and personal - user privacy (Android Enterprise with work profile)" activation type will be out of compliance after the user opens the UEM Client, and the user must change their password to satisfy the configured rules. In the same scenario on Samsung devices with Android 14 or earlier, the user can dismiss the prompt and is not forced to change their password. (EMA-19038)

Samsung devices with an Android Enterprise activation type that are configured to use BlackBerry Secure Connect Plus are not able to use a direct connection to UEM if BlackBerry Secure Connect Plus is not available or if the BlackBerry Connectivity app is not working as expected. This impacts only Samsung devices with one of the following configurations:

- Assigned an Intercede user credential profile and an enterprise connectivity profile with "Container wide VPN" enabled
- Assigned an enterprise connectivity profile with "Per-app VPN" enabled (UEM Client is on the allowed apps list)

(EMA-19034)

After deactivating a Samsung device that was activated with the MDM controls activation type (with the Samsung Knox option enabled), and you try to reactivate it, a "Unknown error: 4025" error message appears if the administrator had assigned a system certificate that's typically pre-installed on the device (such as DigiCert Global Root CA) prior to activation. (EMA-18302) **Workaround**: In the device Settings > View security certificates menu, enable the system certificates (such as DigiCert Global Root CA).
When activating a device in a dark site environment with the Work space only (Android Enterprise) activation type, if the device uses the Samsung SVPN application, it does not activate successfully. (EMA-17497)
On some Samsung devices that were activated on Android 12, the IT policy that is assigned to the device is not correctly applied after upgrading to Android 13. (EMA-17465) **Workaround**: Reactivate the device.
You might not be able to use Knox Mobile Enrollment to activate Samsung Galaxy A52 or Samsung Galaxy XCover devices running Android 11. (EMA-17342)
On Samsung devices running Android 11 activated with the Work space only (Android Enterprise) activation type, Wi-Fi profiles that are configured with a shared certificate are not saved to the device. (EMA-16909)
On Samsung devices running Android 12, if the "Send usage and diagnostic data" setting is enabled on the device but your administrator assigned a policy rule to disable it, the "Based on the admin policy set for your phone, the following policy has been withdrawn: Sending of Diagnostic Data." warning message appears. (EMA-16746)
During activation, the user must set a complex password for the work space even though the IT policy is set to numeric or alphanumeric. (EMA-16254)
When activating a Samsung Knox device, if the screen times out at the Knox license activation screen, the activation is not successful when you try to continue. (EMA-16046)
On some European models of Samsung devices running Android 11, the device Welcome screen appears during activation when using the Work and personal - full control (Android Enterprise fully managed device with a work profile) activation type. The device is activated correctly and the user can follow device setup screens. (EMA-16014)
On some Samsung devices that are activated using the Work and personal - full control (Android Enterprise fully managed device with a work profile) activation type, after upgrading to Android 11, the compliance profile incorrectly restricts apps in the personal space. (EMA-15960)
On Samsung devices activated with the Work and personal - full control (Android Enterprise fully managed device) non-premium activation type, when an administrator unassigns an app, the app isn’t uninstalled but is instead grayed out and cannot be opened. (EMA-14851) **Workaround**: On the device, manually uninstall the app.
If the UEM Client is set as the authentication delegate for BlackBerry Dynamics, and a compliance profile is assigned to users with the "Rooted OS or failed Knox attestation" compliance rule enabled, when the UEM Client is locked due to inactivity and the user enters their password to log in to a BlackBerry Dynamics app, the password is not accepted. The user is returned to the login screen but the password field is greyed out. (GD-67251)

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