



# **BlackBerry UEM Client for Android Release Notes**

12.45.0.158182



# Contents

- What's new in the BlackBerry UEM Client for Android..... 4**
  - BlackBerry Dynamics SDK and BlackBerry Dynamics Launcher versions..... 6
- BlackBerry UEM Client for Android fixed issues..... 7**
- BlackBerry UEM Client for Android known issues..... 9**
- Legal notice..... 11**

# What's new in the BlackBerry UEM Client for Android

## 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)

## What's New in the BlackBerry UEM Client for Android 12.44.0.157998

- **Samsung devices running Android 14:** The UEM Client now supports Samsung devices that are running Android 14 with Samsung Knox 3.10.
- **Device notifications:** Users no longer receive multiple device notifications to install assigned certificates unless a password is required. The UEM Client automatically tries to install certificates in the background, or users can manually import them from the Assigned profiles menu in the UEM Client.
- **Privacy policy:** A link to the privacy policy can now be found on the About screen in the UEM Client.
- **Removed support for Android 10:** Devices running Android 10 are no longer supported.

## What's New 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)

## What's New in the BlackBerry UEM Client for Android 12.44.0.157981

- **Entra ID conditional access enrollment:** Administrators now have the option to make sure that the Microsoft Authenticator app is installed before the user is prompted to start conditional access enrollment when they open the BlackBerry UEM Client. This feature requires BlackBerry UEM server 12.19 QF4. For more information, see [the BlackBerry UEM server 12.19 release notes](#).

- **Show or hide the BlackBerry Dynamics Launcher:** Administrators now have the option to show or hide the BlackBerry Dynamics Launcher in the UEM Client. They can also control whether the tutorial appears when the BlackBerry Dynamics Launcher appears for the first time in the UEM Client. This feature requires BlackBerry UEM server 12.19 QF4. For more information, see [the BlackBerry UEM server 12.19 release notes](#)
- **Device and work profile password requirements:** When users upgrade the BlackBerry UEM Client to version 12.44.0.157981 and later, if the device and work profile passwords do not meet the requirements set by an administrator in the IT policy, users will be prompted to set the device and work profile passwords according to the IT policy rules.

The following Android password IT policy rules are enforced on the device:

- 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.

#### **What's New in the BlackBerry UEM Client for Android 12.43.2.157934**

For Android Enterprise activations, the BlackBerry UEM Client now supports the BlackBerry Connectivity app's ability to establish an HTTP proxy connection when using the secure IP tunnel (BlackBerry Secure Connect Plus).

#### **What's New in the BlackBerry UEM Client for Android 12.43.1.157843**

The BlackBerry Dynamics SDK in the UEM Client was updated to version 12.0.1.79, which includes performance fixes.

#### **What's New in the BlackBerry UEM Client for Android 12.43.0.157801**

- **Support for Android OS 14:** The UEM Client now supports devices running Android OS 14.
- **Android eSIM devices:** The UEM Client now provides additional support for eSIM management capabilities and security improvements.
- **Battery optimization:** The UEM Client now offers better handling of battery optimization for User-privacy activations.

#### **What's New in the BlackBerry UEM Client for Android 12.42.0.157696**

Note that after you have updated your BlackBerry UEM Client, you will need to re-enter your password.

- **Report last BlackBerry Dynamics password change:** The BlackBerry UEM management console can now display the date and time of the last time that a user changed the BlackBerry Dynamics password. This information is displayed in the Managed Device Users grid (Advanced view) and the Device details page.
- **Support for multiple SIMs:** If a device has more than one SIM (for example, a physical SIM and an eSIM), the UEM Client now reports to the BlackBerry UEM server the information for each active SIM on the device.
- **Android eSIM devices:** The UEM Client now supports the option to preserve the data plan on an Android eSIM device when you select the Delete all device data command. By default, this option is selected. The new "Preserve data plan" checkbox is available from both the BlackBerry UEM management console and the BlackBerry UEM Self-Service portal.

- **Support for Google Play Integrity API:** The UEM Client now supports Google Play Integrity to provide additional protection from application tampering.
- **Removed support for Android 9:** Devices running Android 9 are no longer supported.

## BlackBerry Dynamics SDK and BlackBerry Dynamics Launcher versions

Version of UEM Client for Android	BlackBerry Dynamics SDK and BlackBerry Dynamics Launcher versions
12.45.0.158182	BlackBerry Dynamics SDK 13.0.2.143 The BlackBerry Dynamics Launcher is now integrated with the BlackBerry Dynamics SDK.
12.44.0.158016	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.1.1.43</li> <li>• BlackBerry Dynamics Launcher 12.1.590.4</li> </ul>
12.44.0.157998	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.1.1.43</li> <li>• BlackBerry Dynamics Launcher 12.1.590.4</li> </ul>
12.44.0.157991	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.1.0.39</li> <li>• BlackBerry Dynamics Launcher 12.1.590.3</li> </ul>
12.44.0.157981	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.1.0.21</li> <li>• BlackBerry Dynamics Launcher 12.1.590.3</li> </ul>
12.43.2.157934	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.0.1.79</li> <li>• BlackBerry Dynamics Launcher 12.0.0.253</li> </ul>
12.43.1.157843	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.0.1.79</li> <li>• BlackBerry Dynamics Launcher 12.0.0.253</li> </ul>
12.43.0.157801	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 12.0.0.52</li> <li>• BlackBerry Dynamics Launcher 12.0.0.253</li> </ul>
12.42.0.157696	<ul style="list-style-type: none"> <li>• BlackBerry Dynamics SDK 11.2.0.10</li> <li>• BlackBerry Dynamics Launcher 3.6.0.251</li> </ul>

# BlackBerry UEM Client for Android fixed issues

## 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)

### **Fixed issues in the BlackBerry UEM Client for Android 12.44.0.157981**

There are no fixed issues in this release.

### **Fixed issues in the BlackBerry UEM Client for Android 12.43.2.157934**

There are no fixed issues in this release.

### **Fixed issues in the BlackBerry UEM Client for Android 12.43.1.157843**

The BlackBerry Dynamics SDK in the UEM Client was updated to version 12.0.1.79, which includes performance fixes.

### **Fixed issues in the BlackBerry UEM Client for Android 12.43.0.157801**

On Android devices that had BlackBerry Dynamics configured, if the device was not connected to the network when a Remove Device command was issued, the command failed to remove the Work Profile or to factory reset the Android devices. (EMA-17733)

On some devices running Android 13, a user could not select a specific S/MIME certificate for encryption or signing. (EMA-17652)

The PKI-C Library did not comply with RFC 6211 for CMS algorithm identifier protection validation. (EMA-17636)

### **Fixed issues in the BlackBerry UEM Client for Android 12.42.0.157696**

The device could not read the LT value (the time value in long format) in the QR code. (EMA-17581)

On devices running Android 11 and later, when a device was enrolled, the Wi-Fi MAC address was not retrieved and displayed in the Managed Device Users grid (Advanced view). (EMA-17559)

On some Samsung devices with the "Specify Workspace Password and Lock" option enabled, after a user changed the work space password, the API did not lock the work space and the user was not required to enter the new work space password. (EMA-17551)

The UEM Client used a deprecated API to obtain the device phone number. (EMA-17534)



# BlackBerry UEM Client for Android known issues

Issues that are new in this release are noted with an asterisk (\*).

\* On devices running Android 15, the UEM Client app may be reported as a sideloaded app and flagged as a compliance violation even though it was updated from the Google Play store. (MTDLIB-1974)

**Workaround:** Open the UEM Client app on the device.

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.

If a device that is configured for Entra ID conditional access is removed from the Entra endpoint portal by an administrator, and the device is unregistered from the Microsoft Authenticator app, the user is not prompted to authenticate when they switch back to the BlackBerry UEM Client app. (UES-9561)

**Workaround:** Force close the UEM Client and reopen it, or tap **the icon > Settings > Enroll Conditional Access**. Follow the instructions on the screen to authenticate 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 some devices, when the "Specify work space password and lock" command is sent to the device, the password is successfully changed but the work space doesn't lock properly. (EMA-16954)

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)

In dark site environments, on Samsung Galaxy S20 devices running Android 10 activated with the Work and personal - user privacy or Work and personal - full control (Android Enterprise) activation types, the VPN profile is not created on the device. (EMA-16739)

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.

# Legal notice

©2025 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE 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.

Patents, as applicable, identified at: [www.blackberry.com/patents](http://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