Universal Device Service

Version: 6.0

Release Notes

BlackBerry®

Published: 2012-04-05
SWD-20120405181146835

Contents

1 Known issues 4
- Activation known issues 4
- Administration known issues 4
- APNs certificate known issues 6
- Device compatibility known issues 7
- Installation known issues 7
- IT policies known issues 9
- Logging known issues 9
- Mobile Fusion Client known issues 10
- Performance known issues 11
- Profiles known issues 11

2 Related resources 13

3 Legal notice 14

Known issues

1

Activation known issues

To erase the activation history for a device, you must delete and recreate the user account and reassign the device. (DT 3234266)

When an Android device is activated with the Universal Device Service and starts communicating with the server, traffic is high and can exceed 60 MB per day. (DT 3238713)

A user can exceed the Maximum number of activations per device value by one. For example, if you specify the maximum number of activations a user can attempt for a device to 4, the user can successfully attempt to activate their device 5 times. (DT 3267383)

In some circumstances, when a user attempts to activate an iOS device or Android device, the Mobile Fusion Client displays a message that the device cannot be activated at this time. This issue might occur if the Communication Module or Scheduler is unable to connect to the Core Module after the installation process completes. For more information, visit www.blackberry.com/go/kbhelp to read article KB31152. (DT 3427515)

Administration known issues

If you have a Wi-Fi network using WEP encryption, smartphones using iOS 4.3.5 and iOS 5.0.1 will be unable to connect to the network. (DT 2598835)

If the administrator selects Disable data service when roaming, the administrator cannot select Disable background data service when roaming. The device user can override the data roaming setting on the device, but cannot override the background data service when roaming. The device then has background data service when roaming without informing the administrator. (DT 2898406)

Workaround: First select Disable background data service when roaming, and then select Disable data service when roaming. Both IT policies are applied to the device.

If you add multiple application sources with different identifiers into one application definition, the correct application source might not be sent to the device. (DT 3092336)

When you log in to the Administration Console using the username "admin," you receive an error message. (DT 3165140)

Unable to import an SRP authentication file. (DT 3178499).

Workaround: Manually fill in the SRP authentication information.

On the Device Communications settings pane, the Network Configuration request setting and Log request setting are not supported. (DT 3193329)

The Scheduler times out when it requests a batch poke of 10,000 devices. The Request Timeout message is caused because Microsoft IIS restarts itself periodically. When Microsoft IIS is restarting, the Poke Service cannot connect to the Core Module if the Timeout value in Rim.Buds.Service.exe.config is too small. (DT 3193836)

Workarounds: 1. Increase the Timeout settings in the Rim.Buds.Service.exe.Config for all services. 2. Ensure a mixed configuration of Microsoft IIS settings in the applicationHost.config and Rim.Buds.Service.exe.Config files.

In some circumstances, if you specify the Device Ownership value to be either Personal or Corporate, the Device Ownership value will be displayed as Not Specified in the Universal Device Service. (DT 3195239)

When you search for a user account using Microsoft Active Directory, you might not find the user account. (DT 3201806)

Workaround:

1. Open Windows Internet Explorer.
2. Select **Tools** > **Internet Options** > **Connections** > **Lan settings** and deselect **Automatically detect settings**.
3. Click **OK**.
4. Click **OK**.
5. Close Windows Internet Explorer.
6. Launch Windows Services (services.msc).
7. Locate and stop the BlackBerry Scheduler.
8. Right-click the BlackBerry Scheduler and select **Properties**.
9. Click the **Log On** tab.
10. Change the User Account from Network service to a User Account.
11. Click **OK**.
12. Start the BlackBerry Scheduler.
13. Close the window.

If a user has an Android device with a SIM card that has a data-only plan, the device carrier information is not shown in the Administration Console. (DT 3206857)

After the administrator saves the Microsoft Active Directory settings, the Administration Console displays a webpage called uploaddirectory.do, which displays page errors. (DT 322868)

Workaround: Click on the Back button or a link to return to the login.do page.

The user list may not be populated in the Administration Console for administrators using Windows Internet Explorer 8. (DT 3231185)

Workaround: Install Microsoft hotfix 2647516 on any computer running Windows Server 2008 that you use to log in to the Administration Console.

The device report for an iOS device in the Administration Console may incorrectly state that Wi-Fi is not supported or enabled for the device, when it is, in fact, enabled and the device is connected to a Wi-Fi network. (DT 3242877)

Unicode characters do not appear correctly in the Edit Application Source fields in the Administration Console of the Universal Device Service. (DT 3278388)

With some device models, if you send the IT Administration commands Specify device password and lock or Lock device, nothing happens on the device. (DT 3289731)

For the HTC EVO View 4G tablet, the device identifier information and model information are not displayed in the user details or in the confirmation screens for IT administration commands. (DT 3291398)

The Universal Device Service supports IBM Lotus Domino and IBM Lotus Notes users. Use the %DisplayName% variable in the ActiveSync settings to allow Lotus Notes users to log in to IBM Lotus Notes Traveler, which allows ActiveSync to access Lotus Domino. Use Microsoft Active Directory to add the user to the directory. Create one Lotus Notes Traveler profile for all Lotus Notes users that uses the %DisplayName% variable to allow the user to access the Lotus Notes Traveler server. (DT 3338300)

APNs certificate known issues

If the Enhanced Security Configuration (ESC) is enabled or the Security level is set to High in Windows Internet Explorer, the browser does not function correctly when you click Install APNs Certificate on the Get an APNs Certificate screen, in Step 3 | Upload an APNS certificate. (DT 3226512)

If you use Windows Internet Explorer 8 or 9 to download a .pem file in Step 2 on the Get an APNs Certificate screen, a text file is downloaded instead and you receive an error when you try to install the file in Step 3. (DT 3226645, DT 3229176)

Workaround: Re-download your existing APNs certificate directly from the Apple portal and try Step 3 again.

When installing an APNs certificate, the Private key password must not exceed seven characters in length. If it does, the import will fail. (DT 3230416)

Device compatibility known issues

If a user submits the user certificate name that is prompted (prepopulated) on Android devices, the certificate is not linked to the Wi-Fi profile and Wi-Fi authentication will fail. This is an issue with the device, not with the Universal Device Service. (DT 3406200)

Users cannot connect to the WEP Wi-Fi network from Samsung Galaxy Nexus (Android OS 4.0.2) or Samsung Galaxy Tab 10.1 (Android OS 3.2) devices. This is an issue with the devices, not with the Universal Device Service. (DT 3483034)

Users cannot connect to Wi-Fi with TTLS EAP-GTC from iPhone 4, iPhone 4S, and iPad devices. This is an issue with the devices, not with the Universal Device Service. (DT 3485085)

Installation known issues

You cannot install the Universal Device Service on localized Windows operating systems.

If you select the same port for the Core Module and Communication Module, the Universal Device Service might stop responding. (DT 2866394)

If you install the Communication Module as a standalone module and the SSL certificate is invalid, you do not have the option to go back in the Universal Device Service setup application. (DT 2972356)

Workaround: Cancel the installation and start again.

If you are installing the Universal Device Service to a local drive and there are exactly 0 bytes of local disk space available, you are not warned that there is not enough space in the installation folder and instead receive an incorrect error message stating "the setup application is unable to determine the amount of available disk space on a network drive." (DT 2980821)

During installation of the Universal Device Service, if the calculated remaining space is 0, the expected error message does not appear. (DT 2988829)

The Universal Device Service requests the user's credentials every time it is installed, confusing users who may think that a service account is required for the Universal Device Service. User credentials are required only when installing the Core Module using Windows authentication to connect to Microsoft SQL Server. (DT 3164849)

On the Finalize installation screen of Universal Device Service, if the user clicks cancel after a "core unreachable" error message, the installation is not cancelled. The installation continues and does not complete. (DT 3164865)

When you change the password for the keystore files using the Universal Device Service Configuration and click OK, the Keystore settings tab is blank and the password is not saved. (DT 3189071)

Workaround: Click Apply and then click OK.

During installation, the JRE update installation may fail. (DT 3194315)

Workaround: Install JRE 6 Update 31 manually using the command **jre-6u31-windows-i586.exe /s STATIC=1 or jre-6u27-windows-i586.exe STATIC=1**. Do not use the **/L** switch.

After you install the Core Module and the Communication Module on a standalone computer, the Finalize Installation dialog box incorrectly lists components that have not been selected for installation. (DT 3202223)

When you reinstall the Universal Device Service, you must type Client Access License key in the Universal Device Service CAL and SRP information dialog box. (DT 3218781)

If you install the Communication Module on a separate computer, or if you use a custom installation folder, the tabs on the Universal Device Service Configuration window are not visible. (DT 3218807)

When you click Next multiple times before the system finishes processing an action, the installation might not complete successfully. (DT 3223519)

Workaround: Click Next once and wait for the system to finish processing the action.

If the Windows Installer is in use by another process when you begin installing the Universal Device Service, you do not receive a warning message and the installation does not complete successfully. (DT 3228352)

After a reinstallation of the same software bundle, if an administrator creates a custom logs folder, the setup logs and Administration Console logs do not go to the custom logs folder. Instead, they are sent to the original default logs folder. (DT 3356497)

After the Universal Device Service is uninstalled, the empty BlackBerry Mobile Fusion folder remains in the Start > All Programs menu. (DT 3367277)

When the Universal Device Service is installed on Windows Server 2003 SP2 64-bit and Windows Server 2003 R2 SP2 64-bit, which are unsupported environments, no error message appears, and the installation proceeds. (DT 3368096)

To avoid potential installation issues, perform preinstallation tasks before you install the Universal Device Service on Windows Small Business Server 2011. For more information, visit www.blackberry.com/btsc to read KB31074 and KB31062. (DT 3466342)

IT policies known issues

Unable to modify a custom IT policy that is assigned to a group with many users in it. This can occur if you modify the IT policy multiple times in consecutive order. (DT 2995504)

With some Android device models, if a user did not previously have a password set for their device, and an IT policy is pushed to the device that requires the user to set a password, the user cannot set a password. (DT 2997042)

If an Android device user enters an incorrect password more than the number of times allowed by the IT policies, the device is not wiped if the length of the incorrect password is fewer than four characters. (DT 3200385)

When you assign an IT policy to a group, the Universal Device Service might assign the policy only to some of the user accounts in the group. (DT 3242729)

IT policies for password requirements are not enforced on Android devices. (DT 3427848)

Logging known issues

When a log file reaches 50 MB, the Universal Device Service overwrites the file instead of creating a new log file. (DT 3175767)

If you increase the maximumFileSize in the Core Module web config file, and if more than one Core Module log file exists, new logs are appended to the first Core Module log file instead of being appended to the most recent Core Module log, or being added to a new file. (DT 3194960)

The Universal Device Service generates unnecessary error logs in the Core Module and Communication Module log files and in the Device Event History that are related to "action.poke." (DT 3186595, DT 3202087)

When the Universal Device Service restarts, it does not reset or rollover the log files. (DT 3227586)

The logs for the Core Module and Communication Module are moved out of the date folder and into the corresponding component folder, leaving the date folder empty. This usually occurs at 24:00 h when new folders are created. Administrators may not find the log files where they are expected to be. (DT 3238650)

Mobile Fusion Client known issues

When you remove the Mobile Fusion Client from a device, the Universal Device Service continues to send email messages to the device. (DT 3218777)

The About screen of the Mobile Fusion Client for iOS does not correctly show the current activation time. Instead, it shows the time when the device was first activated. (DT 3232876)

When a user installs the Mobile Fusion Client on an iOS device and clicks Done, the user is not directed to the Mobile Fusion Client, but instead sees a blank screen. (DT 3233407)

The steps to uninstall the Mobile Fusion Client are not documented. (DT 3339118)

Workaround for iOS devices:

1. Press and hold the **Mobile Fusion Client** icon for three seconds.
2. Tap the **X** at the top-right corner of the icon.
3. Confirm deletion. The Mobile Fusion Client is removed from the device.

Workaround for Android devices:

1. Navigate to **Settings** > **Security** or **Location and Security** > **Device Administration**.
2. Deselect the Mobile Client (Mobile Fusion).
3. Tap **Deactivate** > **OK**.
4. Navigate to **Settings** > **Applications** > **Manage Applications** > **Uninstall**. The Mobile Fusion Client is removed from the device.

After an iOS device is activated, the Mobile Fusion Client for iOS does not display any information on the Compliance Report screen. (DT 342683)

Performance known issues

When you assign an IT policy to a group with 10,000 or more users, you receive an error message after three minutes stating "The system encountered an error. Try again later." The IT policy will still be assigned as long as there is no latency between the Universal Device Service and a remote database. If any latency exists, however, the IT policy will not be assigned for such a large number of users. (DT 3232882)

When you assign an IT policy to a group with 2,000 or more users, latency greater than 10 ms between the Universal Device Service and a remote database causes the system to time out, and IT policies will be assigned to some but not all users. If latency of less than 10 ms exists, you will receive the error message described in DT 3232882 but the IT policy will be assigned successfully. (DT 3242729)

User information is not correctly displayed when you view a very long list of users with multiple devices from Home > All Users and the Show drop-down list is set to 100. You receive a message asking if you want to stop running a script, and clicking Yes renders the display of the information unreadable. (DT 3428394)

Workaround: Log out and then log in again and set Show to display 25 instead of 100.

Profiles known issues

When you create a Wi-Fi profile and select Enterprise as the security type, you must type a value in the User name for authentication of the network field, or devices will not be able to install the profile. (DT 2515051, DT 2598824)

If you type a space or a character before or after the CN or O value in the Subject field in the SCEP profile, the Universal Device Service does not send the SCEP profile to the device. (DT 2987313)

When using variable injection for authentication, the name of the Virtual Certificate is not updated after the name of the SCEP profile is changed. (DT 3030745)

Workaround: Use the old Virtual Certificate name, however, it cannot be found using the Universal Device Service.

The SCEP profile does not install if the value in the Subject field contains a lowercase cn or o. (DT 3129142)

Workaround: Use uppercase CN or O.

When you create a Wi-Fi profile and select Enterprise as the security type and LEAP as the protocol, Android devices are unable to install the profile. Android devices do not support the LEAP protocol. (DT 3194964)

When you configure the external SCEP settings, assign a SCEP profile, and select Auto as the certificate source, the certificate is not issued to the device. (DT 3212046)

When you add a CA certificate profile or Shared Certificate profile, the window may incorrectly display the message “No profiles exist.” (DT 3228263)

When you apply a profile to a group, the window might incorrectly display the message “No profiles exist for this group.” (DT 3229165)

With some Android device models, if you remove a certificate profile from a device, the certificate is not removed from the device. (DT 3232324)

When you assign a Wi-Fi profile to a user with a Samsung Galaxy Tab with Android OS 2.3.3, the device automatically loses its connection with the Wi-Fi network and you cannot manage the device. (DT 3238869)

You cannot remove a CA certificate profile or a Shared certificate profile from users in the edit profile screen. (DT 3323813)

Workaround: Remove the certificate from each user in the edit user screen.

All certificates linked by Wi-Fi profile must be assigned directly to Android users or they will not be pushed to the device. (DT 3373692)

If you have a Cisco VPN environment and configure an IPsec VPN profile with XAuth-PSK authentication, some non-BlackBerry devices may be unable to store the static XAuth passwords. The user is required to enter the XAuth password each time they enable VPN.

Workaround: To allow affected non-BlackBerry devices to store the XAuth password, you can modify the group-policy attributes of the VPN profile in your Cisco VPN system to include the password-storage enable option. For more information, visit www.blackberry.com/btsc to read KB30353.

Related resources

2

To read the following resources, visit www.blackberry.com/go/serverdocs

Resource	Information
Universal Device Service Release Notes	• Description of known issues and potential workarounds
Universal Device Service Installation and Configuration Guide	• System requirements • Installation instructions
Universal Device Service Feature and Technical Overview	• Architecture diagrams • Description of features and components • Data flows
Universal Device Service Administration Guide	• Instructions for creating user accounts, groups, and administrator accounts • Instructions for activating devices • Instructions for creating and assigning IT policies and profiles • Instructions for managing applications on devices

Legal notice

3

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Apple, iPad, and iPhone are trademarks of Apple Inc. Cisco is a trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Android and Nexus are trademarks of Google Inc. HTC and EVO View 4G are trademarks of HTC Corporation. Domino, Lotus, and Lotus Notes are trademarks of International Business Machines Corporation. Microsoft, ActiveSync, Active Directory, Internet Explorer, SQL Server, Windows Server, and Windows are trademarks of Microsoft Corporation. JRE is a trademark of Oracle America, Inc. Samsung, Galaxy, Samsung Galaxy, and Samsung Galaxy Tab 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 at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM 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 web sites (collectively the "Third Party Products and Services"). RIM 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 RIM 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 RIM 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 RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM 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 RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM 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 RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM 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 RIM OR ANY AFFILIATES OF RIM 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 RIM'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 RIM'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 RIM and RIM 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 RIM.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada