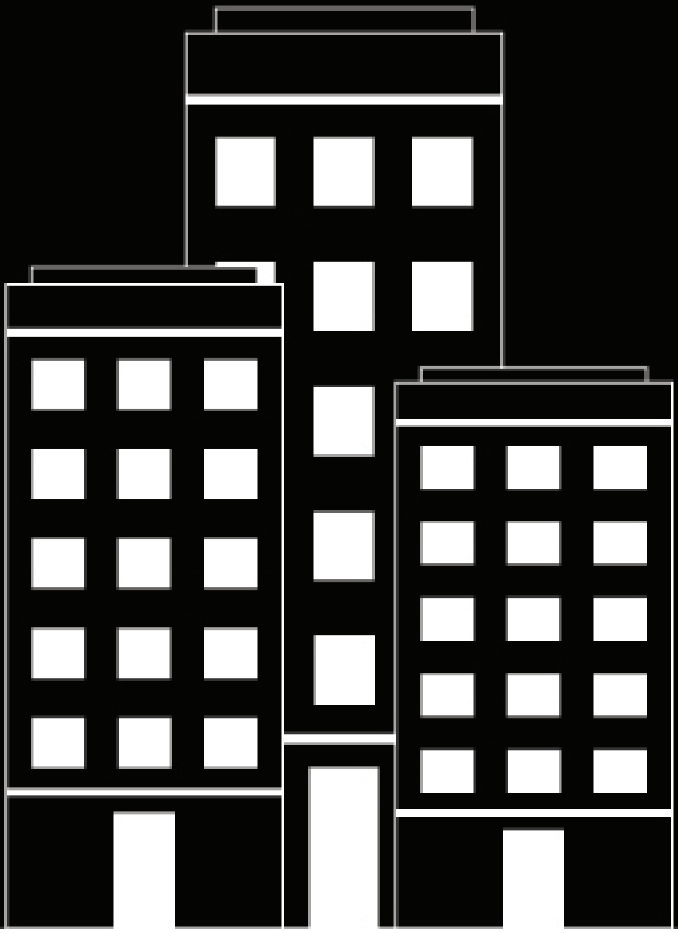

BlackBerry UEM

Release Notes

12.21

Contents

BlackBerry UEM 12.21 and UEM Cloud (November 2024) 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.

Note: Starting in March 2025, BlackBerry will migrate BlackBerry Dynamics services to new domains and IP address ranges. To ensure that there are no disruptions to your BlackBerry Dynamics services, you must update your firewall configuration to allow connections to the new domains and IP ranges, in addition to the existing domains and IP ranges that you have allowed for UEM. For more information, see the new domains and IP ranges for March 2025 and later in the following sections of the UEM Planning Guide:

- Port requirements: Server configuration
- Port requirements: Global IP ranges
- Port requirements: Mobile device configuration

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 12.21 or to upgrade from UEM 12.19 or 12.20. 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.

Fixed issues in UEM 12.21 and UEM Cloud

Management console fixed issues

If you configured UEM to connect to more than one Microsoft Active Directory instance, when you searched for a user account to add from Active Directory, UEM might not have found the user account as expected because it searched the wrong Active Directory instance. (EMM-157231)
You could not assign apps to shared iPad groups when the browser was set to display the management console in German. (EMM-157187)
If you set your browser to display the management console in German, Spanish, or French, when you navigated to Users > Compliance violations, an error message displayed and no devices were listed. (EMM-157122)
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)
Under specific conditions, when you tried to update a hosted internal app, the update might have failed. (EMM-156828)
The DNS Domain Name field in a Managed domains profile did not accept a domain name longer than 6 characters. (EMM-156638)
When you opened an app group, an error displayed indicating that an unexpected error was encountered. (EMM-156584)
If you navigated to the Org Connect section in the management console, a notification message displayed indicating that the Org Connect plug-in requires BBM Enterprise, but the Next button was greyed out. This prevented you from registering Org Connect. If Org Connect was registered previously, you could not manage your connection. (EMM-156520)
In a UEM Cloud environment, if a user's Active Directory password contained certain German special characters (for example, ß or umlauts such as ä, ö, ü), the user could not log in to the management console. (EMM-156454)
In compliance profiles, if you selected "Restricted app is installed", the iOS Journal App was missing from the list of built-in apps. (EMM-156432)
In a UEM Cloud environment, if you made changes to an LDAP directory connection and saved, an error message displayed and you could not save your changes until you uploaded the LDAP server SSL certificate again. (EMM-156343)
In the compliance events view (Users > Compliance violations), if you selected a resolved event and clicked the Ignore button, the event was not removed from the view or added to the list of Ignored events. (EMM-156329)
When you added an app group to a device group with a required disposition and saved, the disposition changed to optional. (EMM-156069)
After you set up Chrome OS device management and clicked on the Network tab for an org unit, an error message might have displayed indicating that the profile could not be retrieved. (EMM-151438)

User, device, and app management fixed issues

If you set the expiration for delete commands to never expire, when you sent commands to delete work or device data to devices, the command expired after 24 hours. (EMM-157180)
In a UEM Cloud environment, BlackBerry Dynamics apps could not retrieve a user certificate using a SCEP profile configured with a dynamic SCEP challenge password. (EMM-157026)
Extra logging information has been removed from Debug logging. (EMM-156885)
When BlackBerry Secure Connect Plus or BlackBerry Proxy 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)
If you assigned a VPN profile to iOS devices with the "Connection type" set to IKEv2, the "Authentication type" set to User credential, and “Enable per-app VPN” and “Allow apps to connect automatically” enabled, “Connect on Demand” was not enabled automatically in the VPN settings on iOS devices. Users had to manually enable this setting on their devices. This is resolved in UEM version 12.21. Create a VPN profile for iOS devices with the configuration above, select “Enable VPN On demand”, and for “Enable per-app VPN”, specify a Safari domain. (EMM-156523)
If a device was out of compliance and the compliance action you configured was untrust, in certain circumstances, UEM removed the IT policy from the device. (EMM-156359)
When you sent the Delete all device data command to a device that was activated with an Android Management activation type, a SQL exception error might have displayed in the management console, but the command executed as expected on the device. (EMM-156357)

Known issues in UEM 12.21 and UEM Cloud

Installation and upgrade known issues

In a UEM Cloud environment, when you open the BlackBerry Connectivity Node console for the first time after an upgrade, an HTTP Status 500 error displays and the console does not load as expected. (EMM-157113) **Workaround**: Refresh the page after the error displays.

Management console known issues

When you navigate to Users > Device vulnerabilities, it may take longer than expected for results to display. (EMM-157303)
If you copy an existing app configuration for an Android app but do not change the name, you cannot save the app configuration. An error message does not display indicating that the name must be unique. (EMM-157288) **Workaround**: Change the name of the app configuration and save.
When you open the app configuration for a BlackBerry Dynamics app, the following error message might display if you try to change a setting in a drop-down list: "An error was encountered. The action cannot be performed." You can dismiss the error and save your changes. (EMM-157224)
If you enable the "Automatically update device OS (supervised only)" rule in an IT policy, when you change the start time, the following error message displays: "An error was encountered. The action cannot be performed." You can dismiss the error and save your changes. (EMM-157223)
When you enable a Chrome OS user in the management console, the user is successfully enabled, but an error message displays indicating that the action cannot be performed. (EMM-157206)
When you view managed devices in the console, for Chrome OS devices, the Chrome OS icon does not display as expected in the OS column. (EMM-157196)
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 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

After you assign an Intercede user credential profile, iPad users do not receive a prompt to activate with MyID. (EMA-18761) **Workaround**: Instruct iPad users to open the UEM Client and navigate to Assigned profiles > Import certificates to scan the Intercede QR code that is shared by the MyID administrator.

Due to a timing condition, when you assign an Intercede user credential profile to an iOS device user and the user activates the UEM Client with MyID, in some cases the derived credentials certificates from MyID are not stored in the native keystore on the device. (EMA-18759)

Workaround: Instruct the user to navigate to Assigned profiles in the UEM Client, hold and swipe down to refresh, then import the Intercede certificate again.

If a user's iOS device is already activated with UEM and you enable that user for Entra ID conditional access, after the Microsoft Authenticator app is installed and the user brings the UEM Client to the foreground, the Microsoft authentication screen is not displayed to the user as expected. This is due to a Microsoft known issue. (EMA-18313)

Workaround: Instruct users to force close the UEM Client and open it again.

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 UEM, the device will be unmanaged and cannot be reactivated or complete a factory reset. (EMA-17549)

If you configure compliance prompts for BlackBerry Dynamics apps for the "OS update not applied" (iOS and Android) or "Managed device attestation failure" (iOS) rules and you set the action for BlackBerry Dynamics apps to block or to delete BlackBerry Dynamics app data, then you remove and reassign the compliance profile, the UEM Client and other BlackBerry Dynamics apps may be blocked or deactivated and removed (depending on the selected action) without prompting the user first. (EMM-156895)

When you assign VPP apps with a user license to Apple DEP devices, if you assign the apps right after associating the VPP license to users, the apps might not install as expected because the app license cannot be retrieved. (EMM-156886)

Workaround: See Microsoft Intune - iOS and iPadOS app installation errors: Could not retrieve license for the app with iTunes Store ID.

If you assign a compliance profile with the iOS "OS update not applied" rule set to provide compliance prompts for BlackBerry Dynamics apps, then you change the compliance action for BlackBerry Dynamics apps from block to delete app data, or from delete data to block, prompts are not provided to the user before the enforcement action is applied. (EMM-156884)

When you configure a device profile with different wallpapers for the home screen and the lock screen and you assign the profile to an iOS device, the wallpaper configuration may not be applied to the device as expected. This issue occurs intermittently. (EMM-155689)

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.

When you schedule an OS update for one or more supervised iOS devices, the update is delivered to devices but is not installed. This occurs intermittently and is due to an iOS known issue. (EMM-152977)

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

If an authentication delegate app is configured in an assigned BlackBerry Dynamics profile, when a device user removes the authentication delegate app from their device and then restarts a different BlackBerry Dynamics app and uses the forgot password option, the forgot password option does not work and the user does not receive an error message. (GD-66829)

Workaround: Instruct the user to install the authentication delegate app again.

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 UEM Client and then open the Microsoft Authenticator app.

Performance

If you enable an encrypted connection and communication between UEM and Microsoft SQL Server, the encrypted connection can result in an increase in the UOS CPU on the computer that hosts the BlackBerry UEM Core. (EMM-155875)

Considerations for Android Management activation types

BlackBerry UEM 12.19 introduced 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	UEM version 12.20 and the UEM Cloud June 2024 update introduces CylancePROTECT Mobile support for devices with Android Management activation types. Any settings and compliance rules available in the management console for CylancePROTECT Mobile for BlackBerry UEM are now applicable to Android Management devices.
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: Preserving a device's data plan is 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

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