Security Note

BlackBerry UEM Cloud

Published: 2017-08-11
SWD-20170811094728638

Contents

Document revision history

1

Date	Description
11 August 2017	Updated the locations of the BlackBerry UEM Cloud primary and backup (disaster recovery) data centers.
22 December 2016	Updated BES12 Cloud product names to BlackBerry UEM Cloud product names throughout the document.
20 July 2016	Updated the following topics to include information about the BlackBerry Connectivity Node: • How BlackBerry UEM Cloud keeps your organization's data private • Security and high availability for BlackBerry data centers • Protecting your company directory information • Data flow: Establishing a secure connection between BlackBerry UEM Cloud and the BlackBerry Connectivity Node

Introduction

2

BlackBerry UEM Cloud is an easy-to-use, low-cost, secure device management solution from BlackBerry that allows you to manage various devices for your organization. You can manage BlackBerry 10, iOS, OS X, Android, and Windows devices all from a unified interface.

BlackBerry hosts this service over the Internet with a reliable and secure infrastructure and many security features that allow you to strike the right balance between offering your employees their choice of device while keeping your business data secure.

BlackBerry UEM Cloud includes the following security features:

- Encryption to keep your data protected while it's in transit
- Access controls to keep your data confidential from other tenants
- Physical security to keep BlackBerry data centers safe
- A software development model that focuses on security
- Security policies and rules of conduct for BlackBerry administrators who manage IT systems
- High availability, disaster recovery, and contingency plans to handle emergencies
- An architecture that's designed to provide a secure link between your organization's mail and content servers and devices
- Tenant control of device behavior using IT administration commands, IT policies, and profiles

Security features of the BlackBerry UEM Cloud infrastructure

3

The infrastructure that hosts BlackBerry UEM Cloud offers many security features that provide security, privacy, and continuity to your organization.

How BlackBerry UEM Cloud protects data stored in BlackBerry data centers

BlackBerry UEM Cloud stores the following data in BlackBerry data centers:

- Your organization's information (for example, your organization's name and location)
- Names and email addresses of users
- BlackBerry device PINs or serial numbers
- Device hardware and software versions
- Device carriers and telephone numbers
- Free space on devices

BlackBerry UEM Cloud doesn't store your organization's email messages, calendar entries, or organizer data sent to and from devices in BlackBerry data centers.

BlackBerry UEM Cloud includes capabilities that help keep your organization's data secure from denial of service attacks, malware, data loss, and compromise of data integrity while the data is stored. These capabilities include:

- Firewalls between BlackBerry UEM Cloud and the Internet
- Access control lists
- Network scanners (for example, intrusion detection systems and intrusion prevention systems)
- Antivirus solutions and antispam solutions
- Solutions for data-loss prevention
- Monitoring by IT security personnel
- Full backup and restore functionality

How BlackBerry UEM Cloud keeps your organization's data private

BlackBerry UEM Cloud helps keep your organization's data private by restricting access to its hardware and software to only the individuals and systems that have valid requirements and business needs. BlackBerry UEM Cloud uses the following methods to help keep your organization's data private:

- Logs and audits all access to the infrastructure. Log files are reviewed regularly by BlackBerry administrators.
- Maps your organization and your organization's users to specific tenants during the provisioning process.
- Allows for directory authentication of administrators and users before permitting the administrators and users to access the BlackBerry UEM Cloud consoles (requires the BlackBerry Connectivity Node).
- Controls access to the management console so that only your organization's administrators or partners can manage your organization's user accounts and devices.
- Controls access to features such as contact lookup so that your organization's users can view only contacts that are part of your organization.

Security and high availability for BlackBerry data centers

BlackBerry data centers are located around the world, and are designed to provide high availability and disaster recovery. BlackBerry data centers provide secure physical access to buildings, monitoring, and hardware redundancies to help protect BlackBerry UEM Cloud from natural disasters and unauthorized access.

BlackBerry data centers have disaster recovery plans for service outages. The plans are designed to have minimal impact on device users. Data and applications are backed up in near real time to avoid data loss.

All BlackBerry data centers have physical access controls in place to protect them from unauthorized access and safeguard against environmental hazards. BlackBerry data centers are geographically distributed globally, and each facility undergoes a thorough risk assessment. Facilities have multiple redundant power supplies, climate control systems, fire suppression systems, and Internet connections. These environments are monitored at all times by a dedicated team and the systems and failover procedures are tested regularly.

Servers and gateways are protected through a combination of antivirus software, enhanced monitoring, redundancy, segregation, intrusion-detection, and intrusion-prevention systems. BlackBerry implements multiple layers of control to protect against distributed DoS attacks. We have deployed both local and cloud-based DoS mitigation technology across our systems.

The table below shows the locations of the primary data centers and backup (disaster recovery) data centers for BlackBerry UEM Cloud. The backup facilities are not active instances of BlackBerry UEM Cloud.

Region	Main data center	Backup (disaster recovery) data center
Americas (Canada, Central and South America)	Canada	Canada
U.S.A.	U.S.A.	U.S.A.
EMEA	Ireland	Netherlands
Asia-Pacific	Singapore	Hong Kong

BlackBerry uses global infrastructure for data traffic that uses BlackBerry Secure Connect Plus. Therefore, data sent using BlackBerry Secure Connect Plus is routed regionally based on the location of the BlackBerry UEM Cloud tenant. All data sent using BlackBerry Secure Connect Plus is encrypted between the BlackBerry Connectivity Node and the device and can't be read as it passes through the BlackBerry Infrastructure.

Security policies and procedures for managing the IT system for BlackBerry UEM Cloud

BlackBerry employs security experts who create security policies that are designed to comply with various international standards and help make sure that IT system procedures meet the security requirements of various organizations. For example, security policies control any changes to IT systems and are designed to reduce unplanned outages. Security policies also control how BlackBerry monitors for and responds to security incidents.

BlackBerry employees who manage the IT system for BlackBerry UEM Cloud use the security policies to help verify that BlackBerry UEM Cloud maintains the security, continuity, and privacy of your organization's data.

Protection of data in transit

4

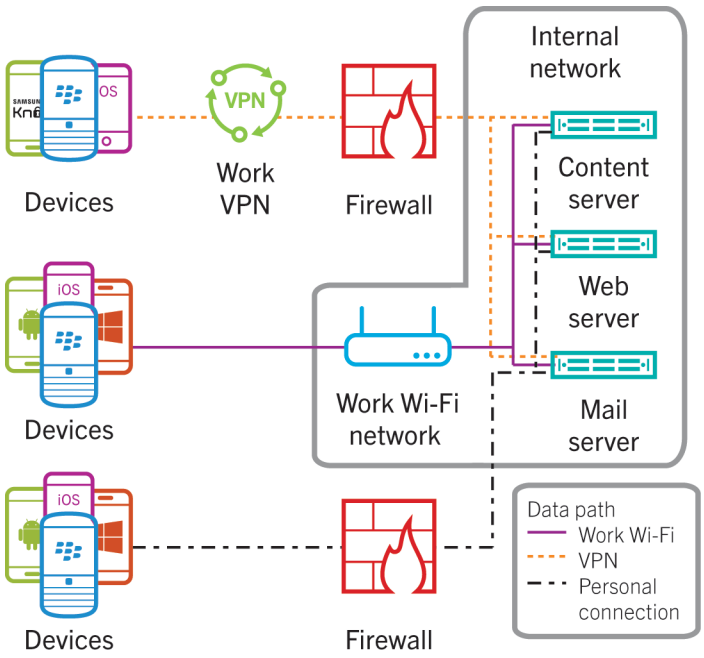
BlackBerry UEM Cloud protects your organization's data in transit using many security methods, such as secure connections and encryption, regardless of the path that data takes.

Protecting data between devices and your resources

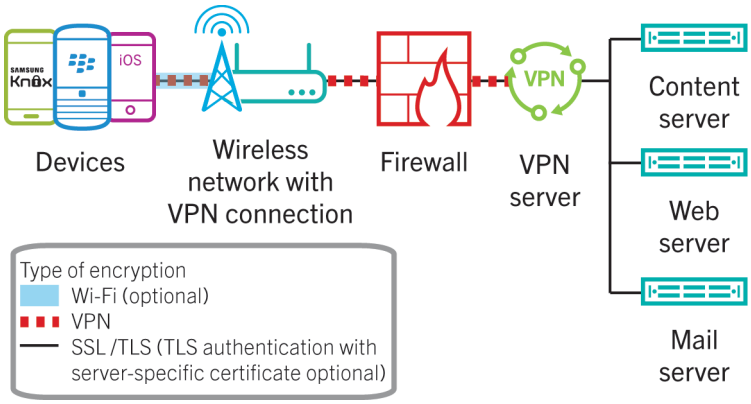
Data in transit between devices and your organization's resources, such as mail servers, web servers, and content servers, is protected by different forms of encryption. The type of encryption used depends on the connection method. By default, devices try to connect to your organization's resources using the following communication methods, in order:

- Work VPN profiles
- Work Wi-Fi profiles
- Personal VPN profiles and personal Wi-Fi profiles

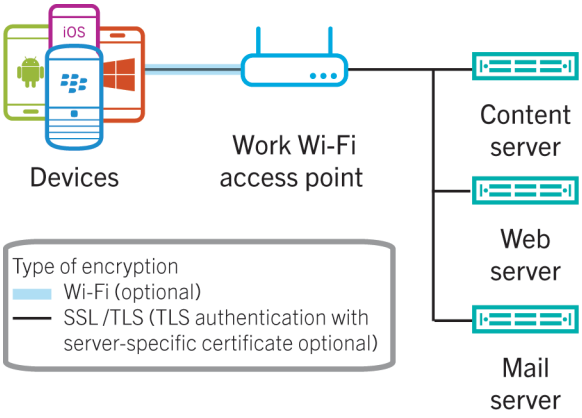
By default, work apps on devices can also use any of these communication methods to access the resources in your organization's environment. The following diagram shows the communication methods that devices can use to connect to your organization's resources:



For data in transit between a device and a VPN server, VPN encryption is used. In a VPN connection, devices connect to your organization's resources through any wireless access point or a mobile network, your organization's firewall, and your organization's VPN server. Wi-Fi encryption is used if the wireless access point is set up to use it. The device can use either password- or certificate-based authentication to connect. The following diagram shows VPN connection encryption:



For data in transit between a device and a wireless access point, Wi-Fi encryption (IEEE 802.11) is used (if the wireless access point is set up to use it). In a work Wi-Fi connection, devices connect to your organization's resources using the settings that you configured in a Wi-Fi profile. The following diagram shows work Wi-Fi connection encryption:



For data in transit between a device and content server, web server, or mail server in your organization, SSL/TLS encryption is used. The encryption for this connection must be set up separately on each server and uses a separate certificate with each server. The server might use SSL or TLS, depending on how it's set up. SSL/TLS encryption is shown in both the Wi-Fi and VPN encryption diagrams above.

Protecting data between apps and your organization's resources using BlackBerry Secure Connect Plus

BlackBerry Secure Connect Plus is a BlackBerry UEM Cloud component that provides a secure IP tunnel for data in transit between apps and your organization's network. This tunnel gives users access to work resources behind your organization's firewall while ensuring the security of data using standard protocols and end-to-end encryption. Depending on the device and configuration, specific apps, all work space apps, or all apps can use the tunnel.

BlackBerry Secure Connect Plus offers the following advantages:

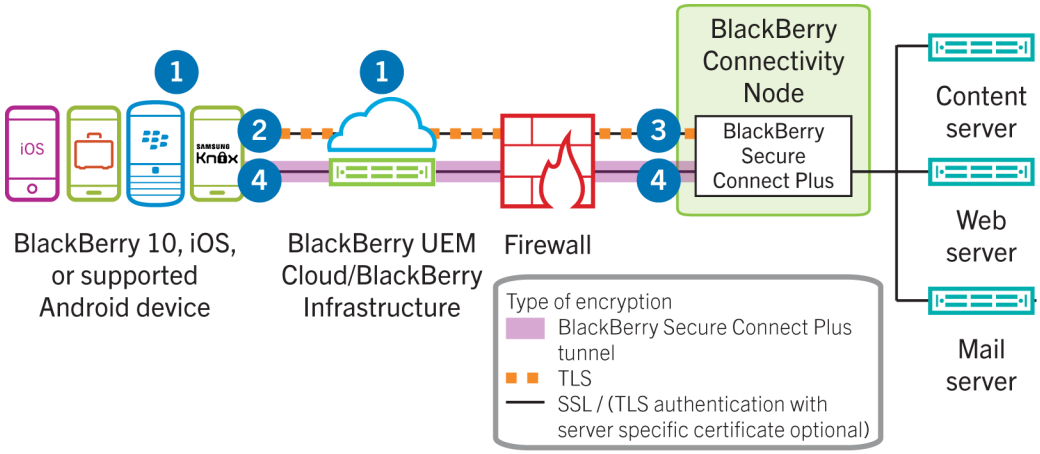
- The IP traffic that is sent between devices and BlackBerry UEM Cloud is encrypted end-to-end using AES-256, ensuring the security of work data.
- BlackBerry Secure Connect Plus provides a secure, reliable connection to work resources without requiring a work Wi-Fi network or VPN.
- BlackBerry Secure Connect Plus is installed behind your organization's firewall, so data travels through a trusted zone that follows your organization's security standards.

For most devices and configurations, BlackBerry Secure Connect Plus and a device establish a secure IP tunnel when a connection to your work Wi-Fi network or VPN isn't available. For iOS devices configured with per-app VPN for BlackBerry Secure Connect Plus, the configured apps use the tunnel even when a connection to your work Wi-Fi network or VPN is available.

After BlackBerry UEM Cloud and the device determine that a secure IP tunnel is the best available method to connect work space apps to the organization's network, the device and BlackBerry UEM Cloud negotiate the tunnel parameters through the BlackBerry Infrastructure. The established tunnel is authenticated and encrypted end-to-end with DTLS. It supports standard IPv4 protocols (TCP and UDP). BlackBerry Secure Connect Plus encrypts and decrypts traffic using FIPS-140 certified BlackBerry libraries with cipher suites for RSA and ECC keys.

Multiple tunnels through the BlackBerry Infrastructure can be created, and each tunnel is for a different device and has a unique ID and DTLS context. As long as the tunnel is open, apps can access network resources. When the tunnel is no longer required (for example, the user is in range of the work Wi-Fi network), BlackBerry Secure Connect Plus terminates it.

Data flow: Establishing a secure IP tunnel using BlackBerry Secure Connect Plus

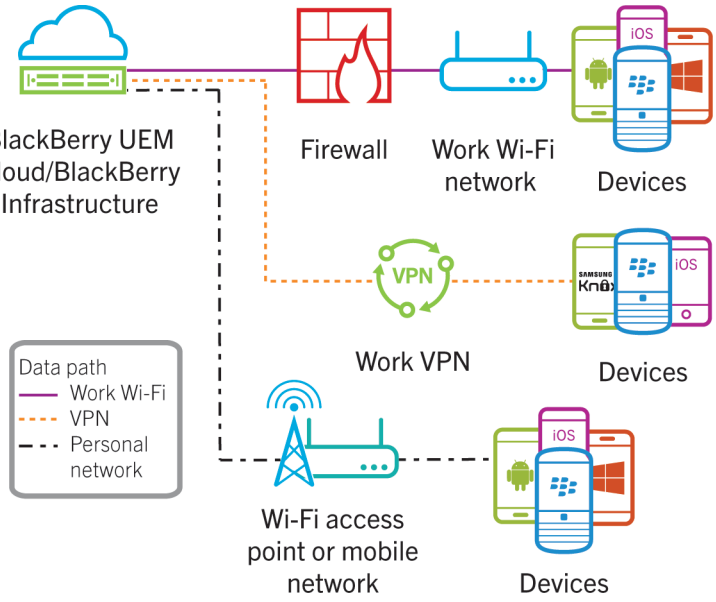


1. BlackBerry UEM Cloud and the device determine that a secure IP tunnel is the best available method to connect apps to your organization's network.
2. The device sends a signal, using TLS, through the BlackBerry Infrastructure to request a secure tunnel to the work network.
3. BlackBerry Secure Connect Plus receives the signal from the BlackBerry Infrastructure.
4. The device and BlackBerry Secure Connect Plus negotiate the tunnel parameters and establish a secure tunnel through the BlackBerry Infrastructure. The tunnel is authenticated and encrypted end-to-end with DTLS.
5. BlackBerry Secure Connect Plus transfers IP traffic (data packets) to and from network resources.
6. BlackBerry Secure Connect Plus terminates the tunnel when it's no longer the best method to connect apps to network resources.

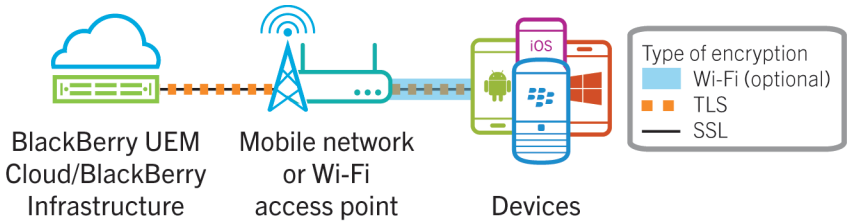
Protecting data between BlackBerry UEM Cloud and devices

BlackBerry UEM Cloud protects data in transit between itself and devices. During the activation process, a mutually authenticated TLS connection is established between BlackBerry UEM and devices.

BlackBerry UEM Cloud sends device management data such as IT policies, profiles, and IT administration commands, to devices and devices send data back to BlackBerry UEM Cloud. This data can travel through a work connection, such as a work VPN or Wi-Fi connection, or a personal connection, such as a personal VPN or Wi-Fi connection. Regardless of the path, the data is protected by client and server certificates over the mutually authenticated TLS connection. The following diagram shows how device management data can travel from BlackBerry UEM Cloud to devices:



The device management data that BlackBerry UEM Cloud sends to devices uses various types of encryption. The following diagram shows the types of encryption used to send device management data to devices:



Protecting your company directory information

The BlackBerry Connectivity Node is an optional component that you can install behind your organization's firewall. It includes the BlackBerry Cloud Connector, which provides a secure connection between BlackBerry UEM Cloud and your company directory, such as Microsoft Active Directory or LDAP company directory, and allows basic attribute synchronization, search functionality, and user authentication services.

BlackBerry UEM Cloud protects your company directory information when it's both at rest and in transit.

BlackBerry UEM Cloud regularly synchronizes user data with the directory, and stores the following information:

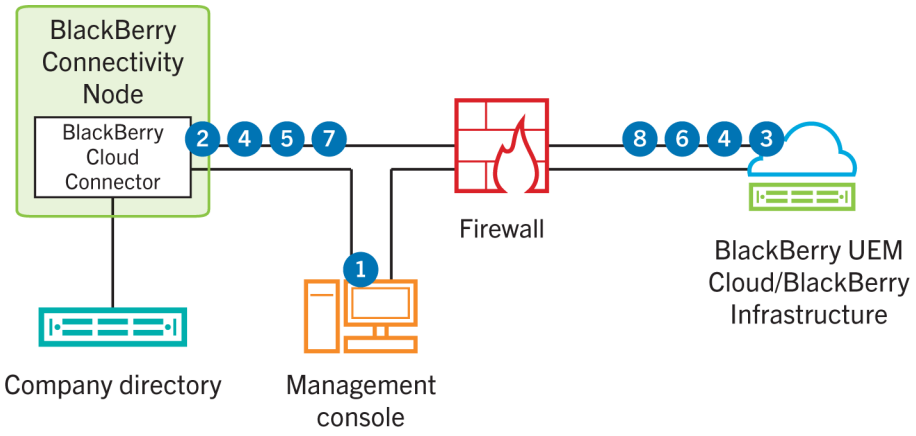
- First name, last name, and display name
- Email address
- User principal name

- Distinguished name
- objectGUID

BlackBerry UEM Cloud never stores user credentials. When a user logs in to BlackBerry UEM Self-Service or the management console, BlackBerry UEM Cloud sends the encrypted credentials to the BlackBerry Cloud Connector for authentication. The BlackBerry Cloud Connector verifies the credentials and sends only a Yes or No response back to BlackBerry UEM Cloud.

BlackBerry UEM Cloud and the BlackBerry Cloud Connector establish a mutually authenticated TLS connection to protect your company directory information while it's in transit.

Data flow: Establishing a secure connection between BlackBerry UEM Cloud and the BlackBerry Connectivity Node



1. You download the installation and activation files from the management console and install the BlackBerry Connectivity Node on a computer that can access the Internet and your company directory.
2. The BlackBerry Cloud Connector component in the BlackBerry Connectivity Node establishes a connection with BlackBerry UEM Cloud and sends an activation request.
3. BlackBerry UEM Cloud verifies that the activation information is valid.
4. The BlackBerry Cloud Connector and BlackBerry UEM Cloud generate a shared symmetric key using the activation password and EC-SPEKE. The shared symmetric key protects the CSR and response.
5. The BlackBerry Cloud Connector performs the following actions:
   a. Generates a key pair for the certificate
   b. Creates a PKCS#10 CSR that includes the public key of the key pair
   c. Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
   d. Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR
   e. Sends the encrypted CSR and HMAC to BlackBerry UEM Cloud

6. BlackBerry UEM Cloud performs the following actions:
    a. Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
    b. Packages a client certificate using your organization's information and the CSR that the BlackBerry Cloud Connector sent
    c. Signs the client certificate using the enterprise management root certificate
    d. Encrypts the client certificate, enterprise management root certificate, and the BlackBerry UEM Cloud URL using the shared symmetric key and AES-256 in CBC mode with PKCS #5 padding
    e. Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the BlackBerry UEM Cloud URL and appends it to the encrypted data
    f. Sends the encrypted data and HMAC to the BlackBerry Cloud Connector
7. The BlackBerry Cloud Connector performs the following actions:
    a. Verifies the HMAC
    b. Decrypts the data it received from BlackBerry UEM Cloud
    c. Stores the client certificate and the enterprise management root certificate in its keystore
    d. Establishes a TLS connection with BlackBerry UEM Cloud
    e. Creates a registration request that includes the tenant ID, the client certificate signed with its private key using SHA-1 and ECDSA, and the time stamp of the signing action
    f. Sends the registration request to BlackBerry UEM Cloud
8. BlackBerry UEM Cloud performs the following actions:
    a. Validates the registration request
    b. Verifies that the time stamp of the signing action isn't older than 3 minutes
    c. Performs one of the following actions:
        - If the validation is successful, registers the BlackBerry Connectivity Node instance and sends the BlackBerry Cloud Connector an authorization token that the BlackBerry Connectivity Node uses for subsequent connections with BlackBerry UEM Cloud.
        - If the validation fails, BlackBerry UEM Cloud closes the TLS connection with the BlackBerry Connectivity Node.

After the BlackBerry Connectivity Node is activated and registration is complete, when BlackBerry UEM Cloud sends a directory request to the BlackBerry Cloud Connector, a mutually authenticated TLS connection is established using the trusted certificates and the authorization token and the BlackBerry Cloud Connector sends your company directory information to BlackBerry UEM Cloud over the secure TLS connection.

Related resources

5

For more information about BlackBerry UEM Cloud, visit http://help.blackberry.com/detectLang/blackberry-uem-cloud.

Glossary

6

AES	Advanced Encryption Standard
CBC	cipher block chaining
CSR	certificate signing request
DoS	denial of service
DTLS	Datagram Transport Layer Security
ECDSA	Elliptic Curve Digital Signature Algorithm
EC-SPEKE	Elliptic Curve – Simple Password Exponential Key Exchange
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards
HMAC	keyed-hash message authentication code
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
PIN	personal identification number
PKCS	Public-Key Cryptography Standards
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UEM	Unified Endpoint Manager
VPN	virtual private network

Legal notice

7

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 Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada