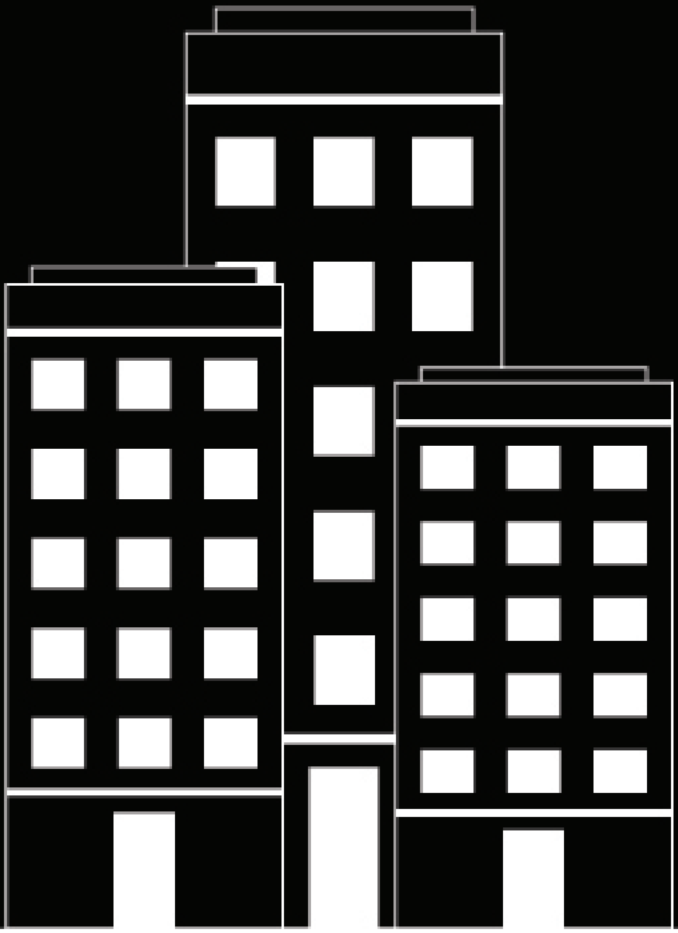

Cylance Endpoint Security

Data Collection Reference Guide

Contents

How Cylance Endpoint Security products collect and use data

This guide provides a summary of how Cylance Endpoint Security products collect, use, and protect user data.

How CylancePROTECT Desktop collects and uses data

For complete information about this product, see the Cylance Endpoint Security docs.

Item	Data collection and use
Malware detection and remediation	• CylancePROTECT Desktop uses machine learning to analyze executable files to: • Prevent malware from executing on device endpoints • Conduct malware risk scoring • Classify malware • Improve the effectiveness of BlackBerry products • The collection of potentially malicious executable files is based on your configuration of the product. You can configure the product to allow or prevent the transfer of the following data: • Hostname • FQDN • IP address • MAC address • File owner • File path • Username • When a potentially malicious executable file is uploaded, it is transferred to the CylancePROTECT cloud services (located in Northern Virginia, US) for scoring. These files are stored separately from your organization's tenant, and any attribution data is de-identified prior to analysis. • BlackBerry does not share collected files with third parties.
Collection of endpoint data	BlackBerry collects and processes the following endpoint data to identify and protect the device from threats: • Hostname • FQDN • IP addresses • MAC addresses • Name of the user most recently logged in

Item	Data collection and use
Data storage and retention	• BlackBerry uses the data described above to facilitate the performance of the license agreement under which BlackBerry’s services and products are offered. The data is shared only with necessary third-party services that are needed to fulfill the intended purpose of the services. • BlackBerry will not sell, lease, or otherwise distribute this information. • Endpoint data is removed at the end of the contract. Administrators can remove data using the management console. • Potentially malicious executables are retained indefinitely. No data is retained that can be used to associate the executable with an individual or organization. • The endpoint data that is collected is stored in Amazon Web Services, in a location of the customer's choice: • Northern Virginia, US • Oregon, US • Frankfurt am Main, Germany • Sao Paulo, Brazil • Tokyo, Japan • Sydney, Australia

How CylancePROTECT Mobile collects and uses data

For complete information about this product, see the Cylance Endpoint Security docs.

Item	Data collection and use
Scanning for malicious apps on Android devices	• The CylancePROTECT Mobile app regularly scans the apps on a user’s Android device. If any apps have a hash that the CylancePROTECT Mobile cloud services (located in Northern Virginia, US) have not previously processed, the .apk files for that app are uploaded. • The CylancePROTECT Mobile cloud services use AI and machine learning to analyze the app package and produce a confidence score that it returns to the CylancePROTECT Mobile app. • The APK files that are uploaded to the CylancePROTECT Mobile services are kept private and anonymous, with no links back to users, devices, or organizations. • The CylancePROTECT Mobile cloud services do not store any user data. The app packages that are uploaded are never shared with a third party. • The CylancePROTECT Mobile app will only upload app files to the cloud services over a Wi-Fi connection. • The CylancePROTECT Mobile cloud services retain app binaries and a corresponding confidence score for security purposes.

Item	Data collection and use
Scanning URLs in SMS text messages for iOS	• When a user receives an SMS text message from an unknown sender that contains a URL, the CylancePROTECT Mobile app sends the message to the CylancePROTECT Mobile cloud services in real time. • The CylancePROTECT Mobile cloud services collect the entire contents of the message. No additional metadata or user identifiers are collected or stored. The data that is collected is never shared with a third party or used by BlackBerry for any purpose other than providing protection from malicious URLs. • The CylancePROTECT Mobile cloud services use advanced machine learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the URL. • New incoming text messages from known contacts are automatically considered to be safe and only messages that contain URLs from unknown senders are scanned and assessed.
Scanning URLs in SMS text messages for Android	• When a user receives an SMS text message that contains a URL, the CylancePROTECT Mobile app sends the unaltered URL to the CylancePROTECT Mobile cloud services in real time. • New incoming text messages from known contacts and unknown senders are scanned and assessed. • The CylancePROTECT Mobile cloud services collect plain text URLs for analysis and assessment. No additional metadata or user identifiers are collected or stored. The data that is collected is never shared with a third party or used by BlackBerry for any purpose other than providing protection from malicious URLs. • The CylancePROTECT Mobile cloud services use advanced machine learning capabilities and accumulated knowledge from threat intelligence feeds to provide an instant assessment of the safety of the URL.
Unsafe network and insecure Wi-Fi checks	On iOS and Android devices, the CylancePROTECT Mobile app will periodically try to connect to the CylancePROTECT Mobile cloud services. If the connection is not successful, CylancePROTECT Mobile determines that the network is not safe. On Android devices, the CylancePROTECT Mobile app periodically checks the properties of the current Wi-Fi access point to determine if it is secure (you can configure which Wi-Fi access algorithms your organization considers secure and insecure). When the CylancePROTECT Mobile app detects an unsafe network or insecure Wi-Fi access point, it is reported in the app and in the management console.

Item	Data collection and use
Endpoint data collection	• BlackBerry collects the following mobile endpoint data to detect and respond to potential threats: ◦ Device name ◦ IP addresses ◦ MAC addresses ◦ OS type ◦ OS version ◦ Device lock screen settings ◦ Device status ◦ Device manufacturer and model • BlackBerry collects the following Android mobile endpoint app data to detect and respond to potential threats: ◦ APK names ◦ APK developer signature ◦ APK binary hash ◦ APK version ◦ APK package name ◦ APK install source • BlackBerry collects the following iOS mobile endpoint app data to detect and respond to potential threats: ◦ iOS developer ◦ iOS signer certificate hash
Data storage and retention	• BlackBerry uses the data described above to facilitate the performance of the EULA under which BlackBerry's services and products are offered. The data is shared only with necessary third-party services that are needed to fulfill the intended purpose of the services. • BlackBerry will not sell, lease, or otherwise distribute this information. • Endpoint data is removed at the end of the contract. Administrators can remove data using the management console. Mobile endpoint configuration and app data are removed 2 months after the end of the contract. • The endpoint data that is collected is stored in Amazon Web Services, in a location of the customer's choice: ◦ Oregon, US ◦ Frankfurt am Main, Germany ◦ Sao Paulo, Brazil ◦ Tokyo, Japan ◦ Sydney, Australia

How CylanceOPTICS collects and uses data

For complete information about this product, see the Cylance Endpoint Security docs.

Item	Data collection and use
Collecting data to detect and respond to threats	• CylanceOPTICS is an endpoint detection and response solution that collects and analyzes forensic data from devices to identify and resolve threats before they impact your organization’s users and data. • You enable a Windows, macOS, or Linux device for CylanceOPTICS by installing the CylanceOPTICS agent alongside the CylancePROTECT Desktop agent. The CylanceOPTICS agent deploys sensors into the OS at various levels and subsystems to monitor and collect a diverse set of data that is aggregated and stored in the CylanceOPTICS cloud database. • You can leverage CylanceOPTICS data in several ways to protect your organization’s environment: • You can query device data to investigate security incidents and discover indicators of compromise. • You can view visual representations of device data to analyze a chain of events. • You can enable detection rules to specify the events that you want CylanceOPTICS to monitor and how you want CylanceOPTICS to respond to those events when they are detected. • The CylanceOPTICS agent sends the device data that it collects to the CylanceOPTICS cloud services. The data is aggregated and stored in the secure CylanceOPTICS cloud database. The CylanceOPTICS data analytics services offer rich interpretations of device data that you can access using the management console. For devices with agent version 2.x and earlier, the CylanceOPTICS database is stored locally on the device. Version 3.0 and later automatically aggregates, stores, compresses, and sends the data to the CylanceOPTICS cloud database at regular intervals. • CylanceOPTICS also offers features that enhance your ability to respond to potential threats. You can deploy packages that remotely and securely run processes to collect and store desired data, you can lock down devices temporarily to prevent the spread of malware, and you can use remote response sessions to execute device commands.
Collection of endpoint configuration data	BlackBerry collects and processes the following information about the configuration of a device endpoint to assess the impact of potentially malicious activity: • Hostname • FQDN • IP addresses • MAC addresses • OS information

Item	Data collection and use
Collection of endpoint process artifacts	BlackBerry collects and processes the following information about endpoint process artifacts to assess the impact of potentially malicious activity: • Name • ID • Image file path • Owner • Command line parameters • Description • Start/end date and time • Parent process • Process attributes
Collection of endpoint file artifacts	BlackBerry collects and processes the following information about endpoint file artifacts to assess the impact of potentially malicious activity: • Path • Creation and last modified date and time • Owner • File hash (MD5 & SHA26) • Alternate data stream information • File attributes • File type
Collection of endpoint user artifacts	BlackBerry collects and processes the following information about endpoint user artifacts to assess the impact of potentially malicious activity: • Username • Username unique ID • Domain • Local group memberships • User privileges • Home directory path • Full name • Account status • Password age • Password status • Country code • Account type • Assigned workstations • Failed login attempts • Roaming configuration
Collection of endpoint registry artifacts (Windows OS only)	BlackBerry collects and processes the following information about endpoint registry artifacts to assess the impact of potentially malicious activity: • Key path • Key values • Referenced file

Item	Data collection and use
Collection of endpoint network artifacts	BlackBerry collects and processes the following information about endpoint network artifacts to assess the impact of potentially malicious activity: • DNS activity • Source and destination IP address • Source and destination port
Collection of endpoint event data	BlackBerry collects and processes the following information about endpoint event data to assess the impact of potentially malicious activity: • File hash (MD5/SHA-256) • File read events • Logon activity • Windows event logs • All WMI events (for example, trace) • Removable media insertion events • Removable media file copy events • Script execution events (JScript, VBScript, VBA macro script, PowerShell) • Name of the user most recently logged in • PowerShell strings (for example, log/pass) • CylancePROTECT Desktop events (threat protection, memory defense, script control)

Item	Data collection and use
Data storage and retention	• BlackBerry uses the data described above to facilitate the performance of the EULA under which BlackBerry's services and products are offered. The data is shared only with necessary third-party services that are needed to fulfill the intended purpose of the services. • BlackBerry will not sell, lease, or otherwise distribute this information. • Endpoint configuration data is removed 30 days after the end of the contract. • Endpoint artifact and event data is stored in the CylanceOPTICS cloud database and is accessible for 30 days. Data is stored in long term backup storage for up to 15 months or 30 days after the end of contract (whichever is less). • In CylanceOPTICS agent 3.0 and later, the data that is collected by the CylanceOPTICS sensors is cached locally before it is sent to the cloud database. If the device is offline, the data is cached until the device can connect to the cloud database. A maximum of 1 GB of data can be stored locally. If more than 1 GB of data is stored before it can be uploaded, the lowest priority data will be deleted so that higher priority data can be cached. • Detections data is stored in the CylanceOPTICS cloud database and is accessible for 30 days. Data is stored in long term backup storage for up to 15 months or 30 days after the end of contract (whichever is less). • InstaQuery data is stored in the CylanceOPTICS cloud database and is accessible for 60 days. • Focus view data is stored in the CylanceOPTICS cloud database for 30 days. • Remote response transactions logs are stored for 30 days. • The endpoint data that is collected is stored in Amazon Web Services, in a location of the customer's choice: • Northern Virginia, US • Oregon, US • Frankfurt am Main, Germany • Sao Paulo, Brazil • Tokyo, Japan • Sydney, Australia

How CylanceGATEWAY collects and uses data

For complete information about this product, see the Cylance Endpoint Security docs.

Item	Data collection and use
Collection of device data	• CylanceGATEWAY collects the following device data to give your organization's administrators visibility into users' network activity: ◦ Hostname ◦ OS ◦ Last connected date and time • The data is accessible to authorized BlackBerry support and service management staff. • Data is retained for as long as a registered device is active.
Collection of endpoint network activity	• CylanceGATEWAY collects the following network activity data from endpoint devices to give your organization's administrators visibility into users' network activity: ◦ DNS activity ◦ Destination IP address ◦ Destination port ◦ TLS certificates ◦ Categories of network resources accessed ◦ Data transferred ◦ Date and time • Administrators can take this data into account when they configure risk mitigation policies. • The data is accessible to authorized BlackBerry support and service management staff. • Data is retained for 30 days.
Identifying alerts and events	• CylanceGATEWAY collects the following information about alerts and events to give your organization's administrators visibility into users' network activity and potential threats: ◦ Risk calculation ◦ Risk type ◦ Status ◦ Username ◦ Device name ◦ Network destination ◦ Action taken ◦ Data transferred ◦ Detection time ◦ Response actions • The data is accessible to authorized BlackBerry support and service management staff. • Data is retained for 30 days.

Item	Data collection and use
Data storage and retention	• BlackBerry uses the data described above to facilitate the performance of the EULA under which BlackBerry’s services and products are offered. The data is shared only with necessary third-party services that are needed to fulfill the intended purpose of the services. • BlackBerry will not sell, lease, or otherwise distribute this information. • The endpoint data that is collected is stored in Amazon Web Services, in a location of the customer's choice: • Northern Virginia, US • Frankfurt am Main, Germany • Sao Paulo, Brazil • Tokyo, Japan • Sydney, Australia

How CylanceAVERT collects and uses data

For complete information about this product, see the Cylance Endpoint Security docs.

Item	Data collection and use
Collection of admin user data	BlackBerry collects and processes the following information about administrators to authenticate authorized administrators and deliver application alerts: • Username • First name • Last name • Email address
Collection of user account data	BlackBerry collects and processes the following information about user accounts to provide application functionality and support service delivery: • Username • User unique identifier • Display name • Email address • User title • User department

Item	Data collection and use
Collection of endpoint data	BlackBerry collects and processes the following information about the configuration of a device endpoint to provide application functionality and support service delivery: • Hostname • FQDN • IP addresses • OS type • OS version • Service packs • Application build • Client type • Processor type • Device unique identifier • Preferred language
Collection of file inventory data	BlackBerry collects and processes the following information from the file inventory to identify sensitive documents and provide the risk assessment: • File hashes • Name of document • Document unique identifier • File type • File size • Device unique identifiers • User with access to the file • Devices with access to the file • Name of the policy that was triggered
Collection of web browser exfiltration events	BlackBerry collects and processes the following information about web browser exfiltration events to mitigate potential data loss: • Date and time of the event • Name of the policy that was triggered • Client source • Application name • Machine learning model • Document name • File type • File hash • Document unique identifier • URL • Page title • File path • File last modified timestamp

Item	Data collection and use
Collection of email message exfiltration events	BlackBerry collects and processes the following information about email message exfiltration events to mitigate potential data loss: • Date and time of the event • Name of the policy that was triggered • Client source • Email client name and version • Document name • File type • File hash • Document unique identifier • Email subject line • Email recipients
Collection of local file transfer exfiltration events	BlackBerry collects and processes the following information about local file transfer exfiltration events to mitigate potential data loss: • Date and time of the event • Name of the policy that was triggered • Client source • Document name • File type • File hash • Document unique identifier • Document source • Document destination • Hostname • Device unique identifier • Username • User unique identifier • Email • Title • Department • File size • Number of policy violations
Collection of file snippets	BlackBerry collects samples of the specific text that triggers the information protection policy. Depending on the configuration of the customer's information protection policies, the file snippet may contain sensitive information, including personal data. This feature is disabled by default.
Collection of evidence files	BlackBerry collects the entire document which contains the text that triggered the customer's information protection policy. Depending on the configuration of the customer's information protection policies, the evidence file may contain sensitive information, including personal data. This feature is disabled by default.

Item	Data collection and use
Collection of administrator login data	BlackBerry collects the login activity from the administrators or operators of customer tenant, including the following information: • Date/time • User unique identifier • Status • Account name
Data sharing or forward processing	BlackBerry uses the identified information to facilitate the performance of the End User License Agreement under which BlackBerry services and products are offered. This data is only shared with necessary third-party services needed to fulfill the intended purpose of these services. BlackBerry will not sell, lease, or otherwise distribute this information beyond what is disclosed below.
Cross-border data transfers	CylanceAVERT customers select the geographic location for their tenant, which is where the personal data that is used to manage the customer’s service and the collected endpoint data is stored. Data is not transferred from the chosen customer’s tenant location to any other geography without customer instruction. The data that is collected is stored by Amazon Web Services, in a location of the customer's choice: • Northern Virginia, US • Oregon, US • Frankfurt am Main, Germany • Sao Paulo, Brazil • Tokyo, Japan • Sydney, Australia
Additional sub-processors	MessageBird: provides a Simple Mail Transport Protocol (SMTP) relay service for email alerts generated by the operation of the product. Collects email address data.

Legal notice

©2023 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.

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