



Cylance Endpoint Security

User Guide

Contents

- What is the CylancePROTECT Mobile app?..... 4**
 - Key features of the CylancePROTECT Mobile app.....4
- Install and activate the CylancePROTECT Mobile app..... 7**
- Enable work mode.....9**
- Enable the message scanning feature.....10**
- Resolve mobile threats.....11**
 - Mobile threats detected by the CylancePROTECT Mobile app..... 13
- Deactivate the CylancePROTECT Mobile app..... 15**
- Report a problem to BlackBerry..... 16**
- What are the Cylance Endpoint Security agents?.....17**
 - Enable work mode in the CylanceGATEWAY agent..... 18
 - CylanceGATEWAY agent settings..... 18
- Legal notice..... 19**

What is the CylancePROTECT Mobile app?

The CylancePROTECT Mobile app provides you with increased awareness of the security of your mobile device and empowers you to take action to resolve threats without administrator intervention.

The CylancePROTECT Mobile app provides you with:

- An overall security assessment of the device
- A list of malicious or sideloaded apps that have been detected
- Alerts about network issues or device settings that pose a security risk
- The ability to detect malicious URLs in text messages
- User-friendly options to guide you to take corrective action, such as uninstall malicious or sideloaded apps and to correct device settings or conditions

The CylancePROTECT Mobile app scans the device in regular intervals to identify threats. When the app detects a threat, you can view details in the app. Whenever possible, the app guides you to resolve a threat and guides you to the device settings where you can address the issue. For more information, see [Key features of the CylancePROTECT Mobile app](#).

Your Cylance Endpoint Security administrator can configure the CylancePROTECT Mobile app to send you a device notification, an email notification, or no notification when a threat is detected. You can always view any active alerts in the CylancePROTECT Mobile app.

The CylancePROTECT Mobile app for Android version 2.3.0.1640 and later notifies you when a new version of the app is available in Google Play. After 30 days, the CylancePROTECT Mobile app will download the update automatically and prompt you to complete the update and restart the app. After 60 days, you cannot use the app until you respond to the upgrade prompt.

The CylancePROTECT Mobile app for iOS supports automatic updates from the App Store.

Key features of the CylancePROTECT Mobile app

The CylancePROTECT Mobile app features warnings that are described in the following tables.

App security feature	Description
Malicious apps	Apps are analyzed to determine whether they are potentially malicious. If you installed an app that is considered to be malicious, the CylancePROTECT Mobile app sends a device notification.
Sideloaded apps	Sideloaded apps are apps that are installed from unofficial or unknown sources are considered to be unsafe because they don't follow the same restrictions or protections as apps distributed through official app stores. The CylancePROTECT Mobile app sends a device notification when a sideloaded app is detected.

Device security feature	Description
Developer options	When developer options are enabled on your device, some sensitive settings and options become available. The CylancePROTECT Mobile app sends a device notification when developer options are enabled.

Device security feature	Description
Root detection	If your device is rooted or jailbroken, it means that you or someone else ran software or performed an action on the device that allows root access to the operating system of the device. You or your administrator might have to remove the rooting software from the device or perform some actions on the device to restore the device to the default state. The CylancePROTECT Mobile app sends a device notification when it detects the device is rooted or jailbroken.
Full disk encryption	Unencrypted data on your device can be easily read by an unauthorized user. The CylancePROTECT Mobile app sends a device notification when encryption is not enabled.
Screen lock	Setting a screen lock prevents unauthorized access on your device, for example, if your device is lost or stolen. The CylancePROTECT Mobile app sends a device notification if a screen lock password or fingerprint has not been set.
Attestation	<p>The CylancePROTECT Mobile app on your device is periodically checked for integrity and authenticity. The CylancePROTECT Mobile app sends a device notification if your device does not pass any of these checks.</p> <p>On Samsung devices, the CylancePROTECT cloud services can also use Samsung Knox Enhanced Attestation in regular intervals to validate the integrity of devices. Knox Enhanced Attestation is hardware-based and can detect device tampering, rooting, OEM unlock, and IMEI or serial number falsification, in addition to performing app health checks.</p>
Device OS	Your administrator might restrict some device OS versions that do not meet your organization's security requirements. The CylancePROTECT Mobile app sends a device notification when it detects the device is running a restricted device OS version.
Device model	Your administrator might restrict some device models that do not meet your organization's security requirements. The CylancePROTECT Mobile app sends a device notification when it detects the device is running a restricted device OS model.

Network protection feature	Description
Wi-Fi security	If your device is connected to a Wi-Fi access point whose network encryption protocol is considered to be insecure, the CylancePROTECT Mobile app sends a device notification.
Network connection	The CylancePROTECT Mobile app evaluates its network connection to the CylancePROTECT Mobile cloud services to determine whether the connection is safe. If the connection is considered to be unsafe, the CylancePROTECT Mobile app sends a device notification.

Message scanning feature	Description
SMS message scanning	When you receive SMS messages that contain URLs, the URLs are scanned to determine whether they are potentially malicious. The CylancePROTECT Mobile app sends a device notification when a malicious URL is detected.

CylanceGATEWAY feature	Description
Work mode	Enable work mode in the CylancePROTECT Mobile app to access network resources safely and protect your device from suspicious and potentially malicious network activity.

Install and activate the CylancePROTECT Mobile app

Before you begin:

- You are ready to activate the CylancePROTECT Mobile app when you receive an activation email from your administrator that contains information to activate the app.
 - Your administrator might have advised whether you are a directory or a BlackBerry Online Account user. If you are a BlackBerry Online Account user and you don't know your credentials, go to the [BlackBerry Online Account password reset](#) page to enter your email address and follow the instructions in the password reset email to set a password that you will use to activate the CylancePROTECT Mobile app.
 - JavaScript must be enabled in your default mobile browser. The CylancePROTECT Mobile app supports Google Chrome, Samsung Internet, and Safari.
1. Download and install the CylancePROTECT Mobile app from the App Store or Google Play.
 2. Open the CylancePROTECT Mobile app.
 3. Review and agree to the BlackBerry privacy notice and terms and conditions.
 4. Do one of the following:

Task	Steps
Activate the app using a QR Code	<ol style="list-style-type: none"> a. Tap Scan QR Code. b. Scan the QR Code from the CylancePROTECT Mobile app activation email that you received.
Directory user: Activate the app with your work email address and password	<ol style="list-style-type: none"> a. Tap Sign in with your account credentials as instructed by your administrator. b. When prompted for your custom domain, type the domain from the CylancePROTECT Mobile app activation email that you received (option C). Tap Next. c. In the Username field, type your work email address. Tap Next. d. In the Password field, type your work email password. Tap Next.
BlackBerry Online Account user: Activate the CylancePROTECT Mobile app with your BlackBerry Online Account email address and password	<ol style="list-style-type: none"> a. Tap Sign in with your account credentials as instructed by your administrator. b. When prompted for your custom domain, type the domain from the CylancePROTECT Mobile app activation email that you received (option C). Tap Next. c. In the Username field, type the email address for your BlackBerry Online Account. Tap Next. d. In the Password field, type the password for your BlackBerry Online Account. Tap Next.
Activate the CylancePROTECT Mobile app using an activation password	<ol style="list-style-type: none"> a. Tap Enter credentials from your activation email. b. In the Custom domain field, type the domain from the CylancePROTECT Mobile app activation email that you received (option B). c. In the Username field, type your username. d. In the Activation password field, type the activation password. e. Tap Continue.

5. Depending on the configuration by your administrator, you may receive multiple prompts to enable and allow access for different features. Complete the prompts and allow access permissions as necessary, and complete any additional instructions that are displayed.

To detect network changes for the Wi-Fi protection feature, you must allow background location permissions all the time.

After you finish:

- You must allow background activity for the CylancePROTECT Mobile app.
- You can repeat these steps to install and activate the CylancePROTECT Mobile app on additional devices.
- The CylancePROTECT Mobile app for Android notifies you when a new version of the app is available in Google Play. After 30 days, the app will download the update automatically and prompt you to complete the update and restart the app. After 60 days, you cannot use the app until you respond to the upgrade prompt.
- The CylancePROTECT Mobile app for iOS supports automatic updates from the App Store.
- See [Enable work mode](#) and [Enable the message scanning feature](#).

Enable work mode



If your administrator configured the CylanceGATEWAY feature for you, you can enable work mode in the CylancePROTECT Mobile app to access network resources safely and protect your device from suspicious and potentially malicious network activity. When you enable the feature, it sets up secure access to analyze network activity and applies network access policies managed by your administrator.

Before you begin: You must allow background location permissions at all times for the CylancePROTECT Mobile app.

1. In the CylancePROTECT Mobile app, do one of the following:
 - Enable the **Work Mode** setting.
 - Tap **Switch on to work safely > Enable work mode**.
2. Tap **OK**.
3. On the **Connection request** dialog, tap **OK** to confirm.

When the connection is established, the "Enabled" status appears.

After you finish:

- If your administrator asks you to enable TCP connections for the CylanceGATEWAY feature, tap  or  on the CylanceGATEWAY screen and select the **Use TCP** option.
- To view warnings about suspicious network activity, tap **View Warnings**. From the **Warnings** screen, you can also choose to mute warning notifications.

Enable the message scanning feature

You enable the message scanning feature in the CylancePROTECT Mobile app to allow it to scan incoming SMS messages for potentially malicious URLs. Only URLs in the messages are assessed.

For iOS devices, only messages from unknown senders (contacts that are not on the device's contact list) are scanned. Messages that contain potentially malicious URLs are filtered to the junk folder.

For Android devices, all messages from known contacts and unknown senders are scanned. Messages that contain potentially malicious URLs are listed in the CylancePROTECT Mobile app but you must delete them manually in the default messaging app.

On your mobile device, do one of the following:

Device	Steps
iOS	<ul style="list-style-type: none">a. Open the Settings app.b. Navigate to Messages > Message Filtering > Unknown & Spam.c. In the Message Filtering section, enable the Filter Unknown Senders setting.d. In the SMS Filtering section, tap Protect.e. Tap Enable. <p>These instructions can also be found in the CylancePROTECT Mobile app from Device Health > Message scanning.</p> <p>If you are using the iMessage app, enable the Send as SMS option in the app.</p>
Android	<ul style="list-style-type: none">a. In the CylancePROTECT Mobile app, tap Device Health.b. Tap Message scanning to expand it.c. Enable the message scanning feature.d. On the Allow message scanning screen, tap Allow.e. Tap OK.

In the CylancePROTECT Mobile app, the "Scanning enabled" status message displays.

Resolve mobile threats

When the CylancePROTECT Mobile app detects mobile threats on your device, you receive a device notification. You can open the CylancePROTECT Mobile app to quickly identify the threats and resolve them.

1. Open the CylancePROTECT Mobile app.
2. Tap **Device Health**.
3. Expand one of the following sections:
 - App security
 - Device security
 - Network protection
4. Use the following table to help resolve any threats that were detected on the device.

Feature	Platform	Description	Resolution
App security			
Malicious apps	Android	Expand the section to display a list of any malicious apps that the app has detected.	Tap Fix to uninstall a malicious app from the device OS.
Sideloaded apps	Android iOS	Sideloaded apps are apps that were installed from unknown or untrusted sources. On Android devices, expand the section to display a list of any sideloaded apps that the app has detected. On iOS devices, expand the section to display a list of third-party application developer profiles that are trusted and installed on your device.	Tap Fix to view instructions for removing the sideloaded app. On Android devices, you are directed to the device settings to uninstall the app. On iOS devices, you are directed to the Settings app to remove the trusted app profile from your device.
Device security			
Developer options	Android	Developer options indicates whether developer mode is enabled on the device.	Tap Fix to view instructions for turning off developer mode. You are directed to the device settings to turn off developer mode.
Root detection	Android iOS	Root detection displays a notification if the app detects that the device is rooted or jailbroken.	No action in the app. You must contact your administrator for a resolution.

Feature	Platform	Description	Resolution
Full disk encryption	Android	Full disk encryption indicates whether disk encryption is enabled on the device.	Tap Fix to view instructions for turning on disk encryption. You are directed to the device settings to turn on disk encryption.
Screen lock	Android iOS	Screen lock indicates whether a screen lock option (for example, a password or fingerprint) is currently enabled on the device.	Tap Fix to view instructions for turning on a screen lock. On Android devices, you are directed to go to the device settings to turn on a screen lock.
Device attestation	Android iOS	<p>On Android devices, a notification is displayed if the CylancePROTECT Mobile app fails any of the following:</p> <ul style="list-style-type: none"> • SafetyNet attestation • Hardware certificate attestation • Hardware attestation security level lower than what is configured in the CylancePROTECT Mobile policy • Hardware attestation security patch level is lower than what is configured in the CylancePROTECT Mobile policy • Hardware attestation boot state is unverified <p>On iOS devices, a notification is displayed if the CylancePROTECT Mobile app fails an integrity check using the Apple DeviceCheck framework.</p>	<p>For Android devices, if the security patch level does not meet the configured minimum patch, tap Fix to check for software updates.</p> <p>For other attestation alerts and integrity checks, there is no action in the app. You must contact your administrator for a resolution.</p>
Device OS	Android iOS	Device OS indicates whether the device OS meets the requirements in the CylancePROTECT policy that is assigned to you.	Tap Fix to view instructions for upgrading the OS. On Android devices, you are directed to the device settings to upgrade the OS.

Feature	Platform	Description	Resolution
Device model	Android iOS	Device model indicates whether the device model meets the requirements in the CylancePROTECT policy that is assigned to you.	There is no action to perform in the app. You must contact your administrator for a resolution.
Network protection			
Network connection	Android iOS	Network connection indicates whether the current network is unsafe.	Tap Fix to view instructions for disconnecting from the unsafe network. On Android devices, there is an option to go to the device settings to disconnect from the network.
Wi-Fi security	Android	Wi-Fi security indicates whether the current Wi-Fi network is insecure.	Tap Fix to view instructions for disconnecting from the Wi-Fi network. On Android devices, there is an option to go to the device settings to disconnect from the Wi-Fi network.
Message scanning features			
Malware messages detected	Android iOS	Identify SMS text messages with potentially malicious URLs.	On Android devices, tap Fix to go to the default messaging app to delete the text messages. On iOS devices, the text messages are automatically filtered to the junk folder.

Mobile threats detected by the CylancePROTECT Mobile app

The following threats can be displayed in the CylancePROTECT Mobile app:

Mobile security threat	Risk level	Color
Malicious apps	High	Red
Sideloaded apps	High	Red
Device security: Developer options	Medium	Yellow



Mobile security threat	Risk level	Color
Device security: Screen lock	Medium	Yellow
Device security: Rooted or compromised device	High	Red
Device security: Full disk encryption	Medium	Yellow
Device security: Attestation	High	Red
Device security: Security patch level	Medium	Yellow
Device Security: Device OS	Medium	Yellow
Device Security: Device model	Medium	Yellow
Network Protection: Network connection	High	Red
Network Protection: Wi-Fi security	Medium	Yellow
SMS message scanning (displayed for Android only)	Medium	Yellow

Deactivate the CylancePROTECT Mobile app

When you deactivate the app, your device no longer receives notifications to warn you about security risks. The CylanceGATEWAY feature will also be unavailable to access work resources and applications.


Before you begin: Make sure that your device is connected to the wireless network.

On the CylancePROTECT Mobile app home screen, do one of the following:

Device	Steps
iOS	<ul style="list-style-type: none">a. Tap .b. Tap Deactivate.c. Tap Deactivate again.
Android	<ul style="list-style-type: none">a. Tap .b. Tap Deactivate.c. Tap Deactivate again.d. Tap OK.

After you finish: Delete the CylancePROTECT Mobile app from your device.

Report a problem to BlackBerry

1. In the CylancePROTECT Mobile app home screen, tap .
2. Tap **Report a problem**.
3. Type a comment about the problem.
4. Tap **Send**.

What are the Cylance Endpoint Security agents?

The Cylance Endpoint Security agents run on desktop computers and are typically deployed by an administrator to be automatically installed on your device. The following table lists and describes the desktop agents and how you use them.

Agent	What it does	How to use it
CylancePROTECT Desktop	CylancePROTECT Desktop detects and blocks malware before it can affect a device.	Your administrator deploys it to be automatically installed on your device or provides instructions to manually install it. CylancePROTECT Desktop runs in the background on your device after you log in.
CylanceOPTICS	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.	Your administrator deploys it to be automatically installed on your device or provides instructions to manually install it. CylanceOPTICS runs in the background on your device after you log in.
CylanceGATEWAY (desktop agent)	CylanceGATEWAY provides secure access to your organization's on-premises and cloud-based resources, services, and applications without requiring a traditional VPN. It also protects devices by allowing your organization to block connections to unsafe and potentially malicious internet destinations.	Your administrator deploys it to be automatically installed on your device or provides instructions to manually install it. You must activate CylanceGATEWAY using your directory credentials or BlackBerry Online Account credentials. After you activate CylanceGATEWAY, you enable work mode from the agent.
CylanceAVERT	CylanceAVERT identifies and categorizes sensitive files that were found in your organization's environment. If these sensitive files are involved in an attempt to exfiltrate the data through various sources (USB or network drive, email messages, or browser uploads), CylanceAVERT can take a remediation action that was specified by your administrator to protect your data.	Your administrator deploys it to be automatically installed on your device or provides instructions to manually install it. CylanceAVERT runs in the background on your device after you log in.

Enable work mode in the CylanceGATEWAY agent

If your administrator configured CylanceGATEWAY for you, you can enable work mode in the CylanceGATEWAY agent on Windows and macOS devices to access network resources safely and protect your device from suspicious and potentially malicious network activity. When you enable work mode, CylanceGATEWAY establishes secure connections between your device and your organization's network, analyzes your network activity, and applies network access policies managed by your administrator.

Before you begin:

- Install the CylanceGATEWAY agent. To download the agent, go to [the BlackBerry Website](#) and scroll down to the Download CylanceGATEWAY section.
 - Activate the agent using your directory or BlackBerry Online Account credentials. For more information about activating the agent, see the CylanceGATEWAY activation email that you received from your administrator.
1. On your computer, open the CylanceGATEWAY agent.
 2. Click **Enable Work Mode**.
 3. Follow the instructions on the screen.

When the connection is established, the "Work Mode Enabled" status appears.

After you finish: You can [configure settings for the CylanceGATEWAY agent](#).

CylanceGATEWAY agent settings

You can configure settings for the CylanceGATEWAY agent. Setting names may appear differently depending on the device OS.

Setting	Description
Deactivate	Click this button to deactivate the CylanceGATEWAY agent. When the agent is deactivated, it can't receive policy updates from CylanceGATEWAY.
Report a Problem	Click this button to send a problem report to BlackBerry.
Use TCP	Select this option to use TCP for connections to CylanceGATEWAY if your organization's firewall doesn't allow UDP connections.
Launch CylanceGATEWAY automatically when I sign in to this computer	Select this option to start the CylanceGATEWAY agent whenever you log in to your Windows or macOS device.
Connect Work Mode automatically when CylanceGATEWAY launches	Select this option to enable work mode whenever the CylanceGATEWAY agent starts.

Important: If you want the CylanceGATEWAY agent to start and enable work mode automatically each time that you sign in to your Windows or macOS device, you must select both the **Launch CylanceGATEWAY when I sign in to this computer** and **Connect Work Mode automatically when CylanceGATEWAY launches** check boxes.

Legal notice

©2022 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.

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